~~SECRET~~

REPORT TO THE STATE SERVICES COMMISSIONER

Intelligence Agencies Review

Simon Murdoch

Wellington
12 October 2009

Table of Contents

Introduction

1 The New Zealand Intelligence Community (NZIC) exists in its current shape because of historical legacies and the ways in which occupational cultures can dictate organisational form. It looks institutionally the way it does today because its member entities grew in stages, a bit like "Topsy", and were modelled on doctrine and precepts taken from overseas partners. If it sometimes acts in ways different from other parts of the New Zealand public sector that is because intelligence, as a state function, requires particular kinds of restrictions on processes and behaviours (see Annex 3). These can give rise to distinctive, sometimes highly tribal, professional cultures within and between the intelligence organisations themselves. Up to a point this is inevitable, and it is not necessarily a problem given the right internal and external accountability frameworks. By and large, in New Zealand, as far as the control of secret agencies goes, we have strong and internationally orthodox external public accountability arrangements; they were validated in a report by Sir Geoffrey Palmer in 2000. That said, anything to do with intelligence attracts close media and civil society scrutiny, and political bipartisanship cannot always be taken as a given.

2 For quite a long period the NZIC was seen predominantly as a foreign intelligence construct; the product was about international events, situations and actors, and mostly used to support the offshore engagements to which successive governments were committed. The principal linkages were those of the External Assessments Bureau (EAB), Directorate of Defence Intelligence and Security (DDIS) and Government Communications Security Bureau (GCSB) to the Ministry of Foreign Affairs and Trade (MFAT) and the New Zealand Defence Force (NZDF). New Zealand Security Intelligence Service (NZSIS) participation was more case-by-case. But that began to change around the 1990s, and more recently the NZIC has been in a period of significant growth and considerable flux, adapting itself, in terms of its membership and its outputs, to the contemporary national security agenda of our government. This agenda embraces shifting New Zealand indigenous or sovereign security concerns, especially in regard (post 9/11) to "homeland security", as well as a variety of new foreign policy engagements with an international or regional security dimension, often collective in nature. On top of this, (and leaving aside some expansion of the vetting and computer network assurance roles NZSIS and GCSB undertake for the wider public sector) s.6(a) [redacted] Significant additional budget, enough to cope overall, if not entirely, with these multiple demand pressures has been available and new capital and operating funding has flowed into the sector's infrastructure and processing machinery. Until now this has involved a bid scrutiny process by Officials' Domestic and External Security Committee (Intelligence) (ODESC(I)) which, by general budget practice, and notwithstanding qualitative changes in Treasury access, may still seem lacking in contestability.

3 By the same token New Zealand's national technical capacity to generate intelligence has achieved some critical mass and our partners have recently made changes that will enable

higher NZIC off take from their flows. The main challenge to the new or contemporary NZIC today lies in whether it can sustain its present levels of productivity across a widening range of outputs driven by stakeholder demands which continue to intensify, without becoming operationally sloppy or intellectually mediocre. In terms of a "return on their investment", offshore partners will expect NZIC to sustain niche contributions of high professional quality. NZIC's value to this and future governments lies in its overall operational consistency in its protective functions and in its offering timely and well-integrated assessments that enable national security decision makers to manage risks, short and medium term to our domestic and external interests. If it performs well, the NZIC can help protect the state and give advantages that negate the limitations of small nations in the modern world.

4 Because of its smallness, and because being Wellington-centric encourages collegiality amongst its senior management cadres, the NZIC, to date, has been largely able to avoid some of the defects of "siloisation" and "over-compartmentalisation" that might develop in a collection of stand-alone agencies of different sizes. In other jurisdictions these same defects are seen as having caused "intelligence failures"; available data was "lost in the cracks" or misdirected or even distorted, with serious public welfare consequences and major damage to international good standing. But this is not to say the NZIC has any "built-in immunity" by virtue of innate collegiality or superior coordination practices running across its organisational structures. The contemporary national security agenda is both wider and more complex than what has gone before; it is inherently more risk-laden and more demanding.

5 Given the emerging need for quite firm and ongoing fiscal restraint, it is only sensible to be asking what could be done, structurally or managerially to assure Ministers about NZIC's future performance. This is the more so because of related reviews that overlap with mine (Wintringham on defining a contemporary national security framework; Domestic and External Security Group (DESG) s.9(2)(a) on the Foreign Intelligence Requirements system; the Working Party on cyber threats, the Defence White Paper, the integrated border initiatives).

The Way Ahead for the Contemporary NZIC; Findings, Propositions, Suggestions

6 From the conversations I and my review support team have conducted with NZIC principals and other stakeholders ideas about ways ahead for NZIC have emerged.

7 Some are generic propositions and suggestions; others are specific. The generic are:

i. Rearticulate the purposes of the NZIC and redefine its membership via updating the 2005 Domestic and External Security (DES) Committee of Cabinet "charter" (and Palmer's 2000 organogram). These are the "founding documents" for the national security system and the integration of the intelligence community within it. This update should identify roles and responsibilities of all those stakeholders in national security who create or consume intelligence as an all-sources product. And it should specify their relationships with the centre i.e. the coordination and integration machinery in terms of the accountability of individuals as well as committees and other collective bodies. In particular reconsider the purposes of ODESC(I) and the Officials' Domestic and External Security Committee (Policy) (ODESC(R)) from two perspectives; the ongoing need to integrate the intelligence community and the national security/emergency response community for broadly operational purposes; and the requirement to govern the intelligence system on behalf of Ministers, at a cross agency level, in terms of setting future direction, determining resourcing/capability priorities and performance-managing.

ii. Codify the connections between the national security agenda (as defined by Cabinet post the Wintringham report[1]) and the capabilities of intelligence products to clarify policy choices and enhance operational results. Measure if possible or at least weigh up carefully the NZIC's systemic capability to sustain quality inputs to national security goals and tasks.

iii. If necessary adjust, but do not lose the balance between those intelligence outputs directed at present risk mitigation and what needs to be devoted to revealing and understanding medium-term trends and intentions.

iv. Ensure, by means of regular Coordinator-convened meetings with all agency heads, that the NZIC as a whole is focussed on the nature of the value-add which different, specialist streams of collection or assessment can bring to particular tasks; manage from the centre to minimise duplication of input, oversubscription of effort and task-creep, whether self-selected or involuntary within agencies.

v. Develop a more dynamic process for priority setting, adjusting and monitoring; don't just impose a hierarchy on a plethora of 'subjects of possible interest' to consumers, but evaluate risk and set/reset collection and assessment tasks, and give to the Coordinator the responsibility to recommend to ODESC either scaled up or scaled down effort across agencies; monitor progress towards achieving in practice greater flexibility of effort.

[1] By this I mean that Cabinet may end up using a new National Security Framework to identify its principal strategic concerns and to define high level outcomes in terms of its highest risk aversion e.g. as between cyber threats to IT infrastructure; imported or home grown Islamic militancy; proliferation security against WMD etc.

vi. Encourage cross-agency flexibility and mobility in the use of human resources, particularly amongst staff whose professional role contributes to "finished" (assessed) intelligence product; a deeper assessment pool should permit a greater level of subject or sector specialisation across NZIC as a whole in areas of enduring importance to New Zealand s.6(a) [redacted]

vii. Guard against bad habits. Under pressure "dodgy" assessments can arise from policy or collector bias/capture. Reiterate the importance of objectivity, integrity and independence in intelligence assessments. Revalidate the role of the Director EAB to lead i.e. quality control a national assessments programme and an all sources current intelligence product that should bear upon national security matters at hand (including economic and trade risks) that should draw upon inputs from across the national security agenda, and be accessible to relevant Ministers/senior officials, and used in formal advice and decision taking. This might require revised TOR for the National Assessments Committee (NAC) (see page 19).

viii. Plan for something akin to an "efficiency dividend" from the NZIC. Require agency heads and their second tier managers to develop plans for cross-agency service delivery in selected areas where savings are clearly achievable and the risks of compromise of frontline effectiveness are manageable. Pooled corporate and back-office functions and shared processing and distribution technologies should be characteristic of the future NZIC. Set savings/reprioritisation targets for NZIC collectively. A framework for this process is set out in Annex 4.

ix. Manage the expectations of NZIC's key offshore partners from the centre more actively; avoid mixed messaging to partners about the NZIC value-proposition, that of a niche contributor with capacity constraints but some high quality competencies. s.6(a) [redacted]

8 There are also some specific suggestions about things not to do, and things to do structurally, which could help accomplish these goals. They go to the present set of arrangements for NZIC governance/authorisation, and performance accountability:

i. There is not a strong case for restructuring i.e. a two or even three agency merger. Major machinery-of-government projects tend to have more hidden costs and longer payoff timelines than foreseen. NZSIS and GCSB would not fit easily together in terms of core outputs or culture and business practice, and both have unique centres of expertise that require specialised training and development regimes. They both collect secret intelligence, but in very different ways, and each has compartmentalising requirements for sensitive information from offshore partners. They already interact effectively on operations and projects where they need to, as the law permits. There is no "high-hanging" operational synergy that it would need a merger to unlock.

ii. It is more likely NZIC, especially NZSIS, will need to find synergies with the "homeland security" agencies (i.e. border/law enforcement/organised crime) in future as part of a contemporary national security agenda. These agencies which have always collected

and used intelligence as part of their domestic missions are now approaching a new threshold of integration as a public sector border cluster. But their targets have become far more globalised, and they are increasingly part of supranational intelligence networks, capable of a range of clandestine operations aimed at both prevention and pre-emption. Getting this new interface right operationally and legally is arguably the higher priority.

iii. There is a case to look at actual or virtual integration on the assessment side. There is no good reason for the Combined Threat Assessment Group (CTAG) to be separate from EAB; their product is essentially the same and their methods identical. Arguably, DDIS, which is embedded in NZDF to meet an obvious need for "seamlessness" between its operational consumers and its intelligence supply especially for Geospatial Intelligence (GEOINT), would nonetheless benefit from being collocated with a larger critical mass of assessment expertise, and its specialised knowledge and 'mil/mil' networking would benefit the whole. The new GCSB premises could accommodate a collocated 'assessment cluster'. It could lead to some production efficiencies including the GSCB translation/interpretation capability which creates semi finished (partially assessed) intelligence on medium term targets. For short term targets, it would help all assessors, including DDIS, to be closer to the 24/7 watch and warn out centre, New Zealand SIGINT Operations Centre (NZSOC) at GCSB headquarters. And the "homeland security" agencies, notwithstanding their more integrated ("seamlessness") requirements, should also be treated as belonging to a virtual "assessment community". Such developments, taken alongside recommendation (vi) above, might lead to a "rebranding" of EAB as the "National Assessment Bureau (NAB)".

iv. The senior officials' committee, ODESC and the DES Committee of Cabinet to which it would normally report on intelligence matters should undertake NZIC governance at the systemic level. This means setting expectations and endorsing priorities (i.e. scale up/scale down) for intelligence outputs; reviewing performance at the strategic level against national security risks, determining institutional capabilities and resourcing levels. On page 43 (paragraph 6) a structure for this – 'ODSEC (G)' is proposed. The Treasury and the State Services Commission (SSC) which have the tools and expertise but have not had the necessary levels of access or familiarity should be core contributors at this level (see Annex 8). But the central agency leadership and ultimate accountability should remain with the CE of the Department of the Prime Minister and Cabinet (DPMC) and operate through a DPMC based unit. Even if, in future, the Prime Minister were not the portfolio Minister for all three agencies, he/she would still be the essential actor on national security issues, and would chair the Cabinet DES Committee.

v. The Domestic and External Security Group in DPMC drives the coordination machinery to accomplish whole-of-government response to national security risk. The Wintringham report, which follows up some recommendations by the Auditor-General in 2005, is likely to propose a methodology and process to better define and integrate the government's national security goals. It may also address roles and responsibilities within DESG. The Intelligence Coordinator, a second-tier position within DESG, has had a limited mandate and limited authority. In other jurisdictions the comparable function has been strengthened in recent years. The evolution of the NZIC and the

recommended need to give direction to future performance and capability in systemic ways argue for a similar strengthening. But it will need to be considered in light of what is seen to be the appropriate span of responsibilities for the DESG Director[2], and having regard to what should continue to be the clear financial control and legal accountability expectations upon agency heads. This consideration will, of course, be sensitive to "what works in Wellington" but it can take advantage of some of the greater clarity of the role and function specification from other jurisdictions, (i.e. where, in the New Zealand system, and in whom, should the accountability for performing the function be located and the authority vested?). Annex 5 offers some options.

vi. In the UK, the Intelligence Coordinator equivalent has responsibility for the "single intelligence account", which I understand to mean that agency budget bids put up through the separate Ministers are scrutinised from a collective angle, and adjustments may be recommended. I am not sure whether, in fact, there is a single appropriation (for multiple agencies). But some closer understanding of how this works, in reality as well as in theory, might yield some practice that could be adapted for NZIC. And there may be closer to home models e.g. the Justice Sector budget management system.

vii. The employment, remuneration and performance management of the Directors of NZSIS and GCSB are not standard. (NZSIS, by law, sits outside the State Sector Act altogether, and, in the case of GCSB, performance review by the State Services Commissioner is precluded). Although sharing a common Minister, the Prime Minister, and, by virtue of chairing ODESC, having greater visibility of performance than either of the other central agencies, the CEO of DPMC has no formal oversight role either. Both agencies do, in fact, behave as part of the state sector/public service in several important respects e.g. their HR and financial management regimes. In the appointment of agency heads recent practice (as with NZDF Chiefs and the Police Commissioner) has been for the Prime Minister to invite the State Services Commissioner to conduct a merit-based process. The momentum is clearly towards both agencies being drawn into the wider public management regime.

viii. To take the next step and "mainstream" performance management, the two Acts could be amended. Alternatively the Prime Minister as Minister and by law, employer, could advise the two Directors that he wishes to introduce a new condition to their contracts of employment to enable regular performance reviews. The State Services Commissioner could then be appointed to undertake them. The present Directors, in my view, would accept this provided the more sensitive activities they undertake nationally, and with international partners, were not put at risk of compromise of the "need-to-know" principle by an overly intrusive review process which forced disclosure on them. I understand that the State Services Commissioner deals with similar caveats in respect of the performance of heads of other agencies who exercise statutory powers. And both agencies have established audit arrangements which are satisfactory to the Controller and

[2] In other jurisdictions, the National Security Advisor (NSA) and the Intelligence Co-ordinator are separate high level positions but all have direct access to the head of government, and are within a DPMC equivalent structure and answerable to the DPMC CEO. However, in Canada the functions are not split. Either way the New Zealand Intelligence Co-ordinator should carry sufficient authority to deal directly with agency heads and when appropriate, Ministers.

Auditor-General. So it should be possible to find a modality. It would need to take account of the proposal in (iv) above for a new ODESC governance configuration.

Appendices

Annex 1: Intelligence Agencies Review Terms of Reference - 27 May 2009

1 The Prime Minister has traditionally taken Ministerial responsibility for the two principal intelligence agencies, the Government Communications Security Bureau (GCSB), and the New Zealand Security Intelligence Service (NZSIS). In addition, within the Department of the Prime Minister and Cabinet (DPMC), the External Assessments Bureau (EAB) has a critical intelligence assessments role. These three entities are the only ones established solely for the collection and/or analysis of intelligence. Whilst other agencies collect and use intelligence in the course of their other roles it is GCSB, NZSIS, and EAB which form the core of the New Zealand Intelligence Community.

2 It has long been recognised that there needs to be effective coordination and oversight at a 'sectoral' level. This is provided via the Officials' Committee for Domestic and External Security Coordination (ODESC), which forms part of the intelligence system. Cabinet has agreed that ODESC, "shall provide oversight and policy direction to, and shall monitor the performance of, the New Zealand intelligence community and individual agencies. The Committee shall ensure there is full and effective co-ordination and co-operation with the New Zealand intelligence community and that there is no unnecessary overlap of activities or responsibilities".

3 Since the terrorist attacks of September 11, 2001, like many of their counterparts overseas, the two key collection agencies, NZSIS and GCSB, have received significant increases in resourcing and staffing. Broadly, both have doubled in size. EAB has remained the same size.

4 Now it is evident that the current economic and financial situation facing New Zealand means that Government spending will be tightly constrained. This applies to the intelligence agencies as well as to other sectors of Government.

5 However, the context and work of the intelligence agencies will not become any easier. It has become increasingly complex following the end of the Cold War and this is likely to be compounded by the international economic and financial situation.

6 The recent line-by-line review highlighted the inter-dependencies between the various components of capabilities required to achieve effective delivery of intelligence and security results. This applies both within and between the intelligence agencies.

7 The line-by-line review process has also exposed the need for further analysis of the contribution of the Prime Minister's three intelligence entities to national security risk management. It is recognised that each agency has its own mandate and inherent operational complexities. Equally, there are linkages and interdependencies between these agencies themselves, and with other domestic and international partners, that must not be overlooked - or over-simplified - in the drive to understand and manage the important tasks associated with New Zealand's national security risks.

8 Arising from the line-by-line review have been questions about what might be the optimal structure for the three intelligence agencies. NZSIS and GCSB have recently indicated

that there might be room for strengthened administrative collaboration. Work is underway in this area. There may well be other efficiencies to be gained. Recent discussions have also highlighted the need for better shared awareness of national security risk management, respective agency priorities and fundamental business and operational drivers.

9 In thinking about the role of the Bureau and the Service, it has become apparent that consideration also needs to be given to the smallest specialist intelligence body, EAB. This is a much more constrained entity, working within a small central agency. There may be an opportunity for more effective delivery through enhanced collaboration with other intelligence community partners, including through different administrative arrangements.

The Review

10 There is a need to examine:

- How we can optimise the effectiveness of our intelligence and security arrangements across the New Zealand intelligence community as a whole;
- How we can extract further efficiency gains from the funding already provided, so as to be able to reinvest those gains back into more effective intelligence and security capability and delivery of results.

11 A review will be undertaken of the structure of New Zealand's current intelligence activities, to assess whether the present configuration across three agencies is optimal, or whether an alternative arrangement would be preferable. The Review will examine the three core intelligence agencies and assess whether their current structures and modes of operation are optimal for the Minister, and the government as a whole.

12 The review may, as appropriate, examine linkages with other agencies which generate or use intelligence, and may consider coordination mechanisms including ODESC(I).

13 The review will determine whether there are practical options for change in the way the intelligence agencies work to improve overall intelligence outcomes.

14 The Review will be undertaken under delegation from the State Services Commission acting in terms of his functions in section 6(a) of the State Sector Act 1988 and, in respect of the NZSIS, at the invitation of the Prime Minister in terms of section 11 of the State Sector Act 1988. Funding will be sought from GCSB and NZSIS to cover the costs of a suitable reviewer. A contribution will also be sought from DPMC.

15 Simon Murdoch will be appointed as reviewer by the State Services Commissioner. The aim is to conclude the review by 30 September 2009.

16 The reviewer will work with the relevant CEs to establish an effective process for the review. This may include inviting the relevant CEs to form a steering or reference group, and seeking whatever participation or assistance is needed from DPMC, SSC, or the Treasury.

17 This Review will take appropriate account of separate Review of National Security and Intelligence Priorities presently being undertaken by Michael Wintringham, and also further ongoing Review of Foreign Intelligence Requirements.

18 The Review will not address matters such as the functions or powers of the Bureau and Service. They are out of scope for this exercise. Any administrative and/or structural options for improvement that might be suggested by the reviewer will need to recognise and support the distinct roles, functions, and powers currently allocated to each agency.

Annex 2: History

1 Intelligence of all kinds, but especially secret intelligence (revealing concealed intentions, and gathered so as to avoid detection) is a means to an end. It enables the nation state and its institutions to manage risk by discerning policy choices that are better judged because the decision-makers are better informed. It represents the difference between being ill-sighted or even blind to risk and being at least forewarned. It enables pre-emption or at least mitigation to be planned. It facilitates defensive and offensive state behaviour across a full range of national interests.

2 But intelligence has to be interpreted correctly; its meaning is not always easily understood when it arrives in its raw form as bits and pieces of human discourse or bureaucratic data, and it has to be constantly and skilfully contextualised in the assessment process. It also has to be communicated coherently and distributed efficiently to decision-makers so that it can helpfully influence choices about posture and state behaviour. That implies the need for well-managed organisations which understand their business, which engage effectively with each other (the national "intelligence conversation"), and which can not only meet the public accountability standards required of a responsible intelligence culture, but also deliver their outputs professionally.

3 Many countries adopt an 'all-sources' approach to intelligence assessment, they deliberately bring together information collected by a variety of actors in a variety of ways (from totally open sources, from the exchange of diplomatic confidences, from clandestine methods). The requirement for 'current' (tactical) intelligence to inform the short-run event and issue management decisions of the state is a constant. In certain high risk situations intelligence must pass between collectors, assessors and decision-makers in the real time of one telephone call or email exchange. This requirement is balanced by the need for strategic intelligence, to discern deeper trends and to illuminate the likely direction of attitudes and intentions in the medium term, and to clarify long run investment options e.g. defence equipment.

4 So the collection spectrum for an all-sources system which aspires to operate at both the current (real time) and strategic levels is potentially very broad. And it can be investment intensive, the more so when access to some targets is hard to achieve or hard to sustain. In the multimedia age, the proliferation of data-carrying technologies and the spread of affordable electronic communications systems have meant that national intelligence organisations s.6(a) [redacted] still need to do a lot of sifting to find the relevant grains of valuable intelligence.

5 A national intelligence system and apparatus that covers this spectrum is beyond the reach of many countries as a standalone capability. As a general rule, the richer and bigger the country the larger its intelligence capability. The exceptions are states which perceive themselves to be in continual existential danger from without or from within (for them intelligence is core to survival and they will never under invest in it) or those few which can get scale via relationships and networking. There are considerable benefits from the networking of national intelligence systems. These have often been part and parcel of

wider collective security structures and treaties. There is, however, no United Nations (UN) intelligence system per se, and even Interpol has been said to have difficulty effecting exchanges between national police databases. Intelligence overall has been, and is still, the preserve of nation states, and intelligence diplomacy is mostly conducted bilaterally or in small networks.

6 s.6(a) [redacted]

7 In some respects our system is still 'young' by the standards of other countries, and some of its professional capabilities are still maturing. It is possible to think of reasonably distinct evolutionary phases in which the balance between the offensive and defensive needs of the state has shifted and our governments accordingly needed intelligence for new purposes. Within each phase the character, configuration and technical sophistication of the individual components of NZIC adapted and changed. These phases were (i) 1939-45 wartime (known enemies and home front risks, enemy aliens etc); (ii) 1948-1960s Cold War depths (ideological threats and military brinksmanship East/West competition, subversion and state-level espionage); (iii)1964-84 era of containment and superpower mutual deterrence emerging Pax Americanus in Asia, the breach with ANZUS, state-sponsored terrorism; (iv) 1985-2001 collapse of USSR unipolarity/multipolarity, an assumed 'peace dividend', failed state syndrome, including in our Pacific near neighbourhood, WMD proliferation; and (v) 2001 onwards Rogue state syndrome, borderless threats, non-state terror and asymmetric capabilities, globalised financial flows, transboundary criminality, civilisational friction, resource rivalry and energy brinksmanship.

8 In the machinery-of-government sense, management of the New Zealand system throughout the first four phases lay with the same small tight group of agencies MFAT/NZDF-MOD/EAB/GCSB and NZSIS, all being both collectors of intelligence and/or customers for it. They were also responsible, more individually than collectively, for the relationships with 5-Eyes partner agencies. The predominant policy focus was offshore (less so NZSIS whose involvement tended to be more episodic, case-by-case) and the product dealt with international or regional developments in which past governments had active or passive interests. It could be said, with some justification, that the system had an historic bias towards delivering intelligence about international diplomatic and defence relations and managing external partnerships.

9 For many years the SIGINT function was embedded in NZDF; even when it was made autonomous, it remained a secret organisation undeclared to Parliament. The authorisation regime for NZSIS was similar. The retention of the NZSIS and GCSB portfolios by

successive Prime Ministers underlined the tightness of the traditional NZIC, reflecting not just the domestic sensitivity of some functions, s.6(a) [redacted] which were even more than normally sensitive during the two decades of sanctions related to the ANZUS/antinuclear dispute.

10 The creation of the Department of Prime Minister and Cabinet (DPMC) in 1990 brought some change. The leadership of the community moved away from the original group of agencies and towards the DPMC, specifically the DESS coordination machinery which reported through the CEO. The appointment of a dedicated Intelligence Coordinator to DESG, and the development of new external oversight institutions (for legality and propriety of the two secret agencies) in the early 1990s were signals of wider changes in the public policy climate around intelligence and its contemporary purposes. This extended to a new and wider view of national security and security risk management and was given greater force by the events of 9/11.

11 A range of agencies which had always possessed some embedded in-house intelligence capability to meet mission demands for law enforcement and border protection found themselves needing, increasingly, to access non-NZ intelligence in order to be effective at home and in various global or regional partnerships activated to cope with terrorism and other transborder challenges: globalisation's dark side. For these departments (and Crown Entities) the frontline for homeland security has kept shifting further offshore and foreign intelligence has become as important as domestic. The nature of the security risks they seek to manage requires higher levels of interoperability, and greater seamlessness of information and communication amongst them. Their incorporation within the NZIC as customers of finished intelligence is now pretty much an established fact, and their ability to contribute to national assessments (both current and strategic) is recognised in the coordination practices led by DESG as well as institutionally via CTAG and the National Maritime Coordination Centre (NMCC). They should play a full part in the "intelligence conversation" (see Annex 7). Building appropriate frameworks for their operational engagement with the traditional collectors, especially NZSIS, involves some complexities and is more a work in progress.

Annex 3: NZIC Culture and Doctrine: Formative Influences

1 The following points are an attempt to capture some of the received wisdom, s.6(a) [redacted] and the "givens" about intelligence as a profession which, taken together, have influenced not only the cultures of the agencies themselves, but their organisational shape. They may also determine what sorts of inhibitions may exist when it comes to cross-agency collaboration, especially on shared services where the service being provided is in close support of frontline operations, rather than as a corporate input to the organisation. Of course nothing is immutable, and, as seen in other jurisdictions, contemporary needs are forcing a revisiting of established intelligence sector precepts, particularly those that over-compartmentalise technical expertise or skill specialisations, and thus reinforce siloisation. In any event, in order to make sensible choices about future governance and performance management for the NZIC, some awareness of these "legacy" influences on culture and doctrine in the New Zealand system may be helpful.

2 As the Australian Inspector-General has said, intelligence agencies are permitted, subject to conditions and in certain circumstances, to "do things which we do not allow other parts of public administration to do". They can intrude on privacy of information and property; they can conduct activities that would breach the laws of evidence. Many intelligence activities necessarily occur under conditions of secrecy and agency staff must accept higher security obligations about their work and themselves than other public servants. Some elements of intelligence work cannot be detailed in the public domain without impairing future operational options or damaging wider international relationships with partner governments. HUMINT in particular functions around "ironclad anonymity" and guaranteed protection of identity of sources.

3 The core assumptions underlying NZIC's formation and evolution include the following:

- There are significant limitations on the capacity of a Minister or Ministers to direct an intelligence agency or work unit operationally (because of the perceived temptation for the agency resources or information to be commandeered for inappropriate political purposes) and statutory independence acts as a direct constraint.
- There ought to be a degree of reticence in the flows of information between an agency head and the Minister concerning operational methods, sources and other such specifics (a Minister may answer to Parliament he "was not briefed" or "for security reasons, would not comment" or had no need to know.)
- But the Minister must be able to assess the national good and the public interest, and the agency head should not keep from the Minister information, whether of a policy or operational nature, which would better enable the Minister to arrive at balanced judgements and good decisions.
- The public interest in legal compliance and propriety of professional conduct in and by the agencies and their Ministers in the exercise of their powers must be served by the agencies themselves through their business practices and by their visibility to robust scrutiny by legally protected and independent oversight.

- The apparatus and machinery for intelligence collection and assessment should be nationally controlled and it should be capable of interpreting intelligence derived data for New Zealand from New Zealand perspectives.
- Collection and assessment are "sides of the same coin", but inherently different functionally; they utilise distinct professional skills and the managers need different authorising knowledge in order to effectively carry out tasking as well as administrative control functions.
- SIGINT and HUMINT operations employ such different techniques and utilise such distinctive technical skills that they belong in separate organisations. They must comply with separate legal requirements for intercepting the communications of foreign persons, and those of citizens/nationals and for use of the product.
- The domestic outputs of a security intelligence organisation should be differentiated from the related outputs of law enforcement entities whose intelligence product will be tested adversarially and publicly in the courts, and must meet the laws of evidence.
- Assessment of collected intelligence ought generally to be undertaken in a "pure" environment where the risks of capture (whether by collector bias or policy predetermination, or even operational impatience) can be minimised.

4 The NZIC as it is today was shaped by the application of these precepts, which were adapted to both our size and our public sector environment. Unlike Australia and other 5-Eyes, we have not created technology-specific collection entities. GCSB collects and receives SIGINT as well as GEOINT; and it operates the 24/7 watch and warn out system. NZSIS collects domestic security intelligence and foreign HUMINT, besides issuing terrorist and other threat assessments via CTAG. EAB has the mandate to s.6(a) [redacted] to collect "open source" foreign data, and lead the programme of all sources national intelligence assessments. There is embedded collection and assessment capability in NZDF within force units as well as, at both the current/operational level (in Joint Force headquarters (JFHQ)) and the NMCC which it hosts) and at strategic level in DDIS. All agencies in this traditional community issue their own products s.6(a) [redacted] they have received from counterpart agencies.

5 Increasingly other agencies, especially those with law enforcement and border protection mandates are collecting and/or receiving (sensitive) information and intelligence-based assessments from their offshore counterparts. They transform this in-house and issue it under their own "brand". These assessments contribute to national security decision-making. The extent to which they are already tasked on a whole-of-government basis, or could make capability available for shared outputs is a matter for further exploration (the Wintringham report), but it would be a good start anyway to redefine the NZIC with the contemporary and traditional actors all included.

6 EAB has significant responsibilities for a stronger contemporary NZIC. It is the main repository of New Zealand's accumulated intelligence knowledge, and it is a source of specialised expertise on subject areas of special significance in both a national security

context and in terms of contribution to partners (e.g. the Pacific forum region). It has been responsible for three main types of national, i.e. collective – intelligence products:

- It delivers an annual programme of formal national intelligence assessments, developed on an all sources methodology and consistent with accepted standards for objectivity and evidence based judgements. The TOR for the National Assessments Committee, which oversees this programme may be in need of revision in order to fully and appropriately encompass the wider national security agenda and engage all relevant agencies as contributors.
- It produces a digest or bulletin of current intelligence twice a week. This is the product most regularly read by Ministers and senior officials involved in national security issues. It would be worthwhile to revaluate the content boundaries of this material to ensure that it more often picks out – from all sources – the intelligence product that relates to matters of significance to current national security interests and preoccupations. In particular the border security/law enforcement agencies should expect to contribute their intelligence based reports to this EAB product rather than simply use it for in-house purposes or for briefing of their Minister or Ministers.
- EAB produces assessments under its own authority which normally respond to the declared high priority topics under the Intelligence Requirements system. They may also be triggered by the situational requirements of particular customers.

7 EAB maintains a database of 'deep' information which it seeks to have constantly refreshed by its core analytical staff (e.g. its biography series). Ensuring that this database is available to, used by and contributed to by the wider contemporary NZIC will be an important task.

8 In suggesting that it is important for future quality of performance across the NZIC to have at least as much focus on capacity for assessment as on collection, and on a better structured "intelligence conversation" across a virtual assessment community, the obvious entity to build around is EAB, and the obvious standard bearer and point of authority is the Director. Arguably it is time to move on from a title that limits the organisation to 'external' assessments. Perhaps it would be a good signal to rename EAB in a way which ensures its position at the centre of a wider interagency pool of assessment capacity is both understood and acknowledged. If it should prove possible to bring EAB, CTAG and DDIS physically in one location, s.6(a) [redacted] over time, this pool should be able to assure the government of better quality in formal national assessments (e.g. for the next Cabinet consideration of the Government's position on Afghanistan) and deeper expertise across more key areas than is currently possible.

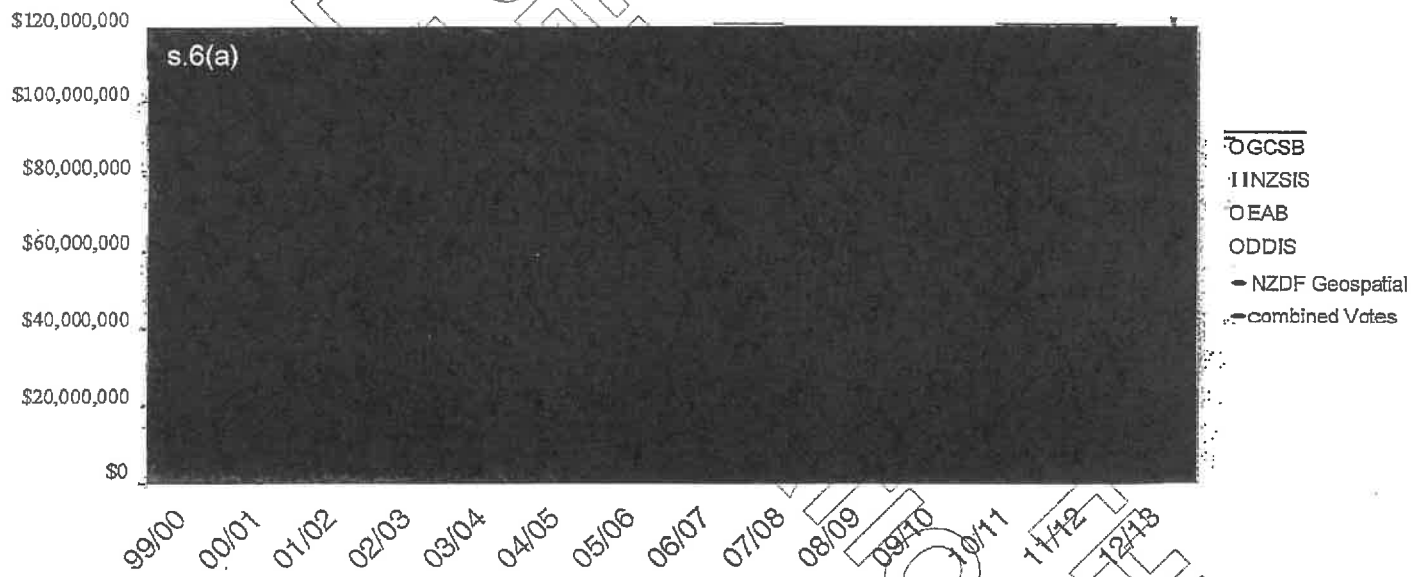
Annex 4: Resourcing; Budgets, Savings and Future Efficiencies

1 This annex attempts to give an overview of the flow of operating and capital funding into the traditional NZIC since 1999. However, it does not incorporate any estimate of DPMC-DESG costs, s.6(a) [redacted] It also leaves aside the intelligence contribution made by parts of NZDF other than DDIS and the new Geospatial unit.

2 It depicts a steady increase in operating budgets across all agencies over the 1999-2009 decade. Both NZSIS and GCSB have had access to regular capital injections over the same period. By FY2013 on current out year numbers, which foreshadow a levelling off of the trend lines, the aggregate outlay for NZIC will be $103m.[3]

[3] It is worth considering this level of expenditure not just as a cost in budget terms but in the context of the annual 'subscription' paid by New Zealand to belong to the 5-Eyes community whose annual capital investment an operating outlays would dwarf ours. It helps explain why the niche contributions that we can make to 5-Eyes burden-sharing are so important and why agency heads strive to be responsive to partner demand.

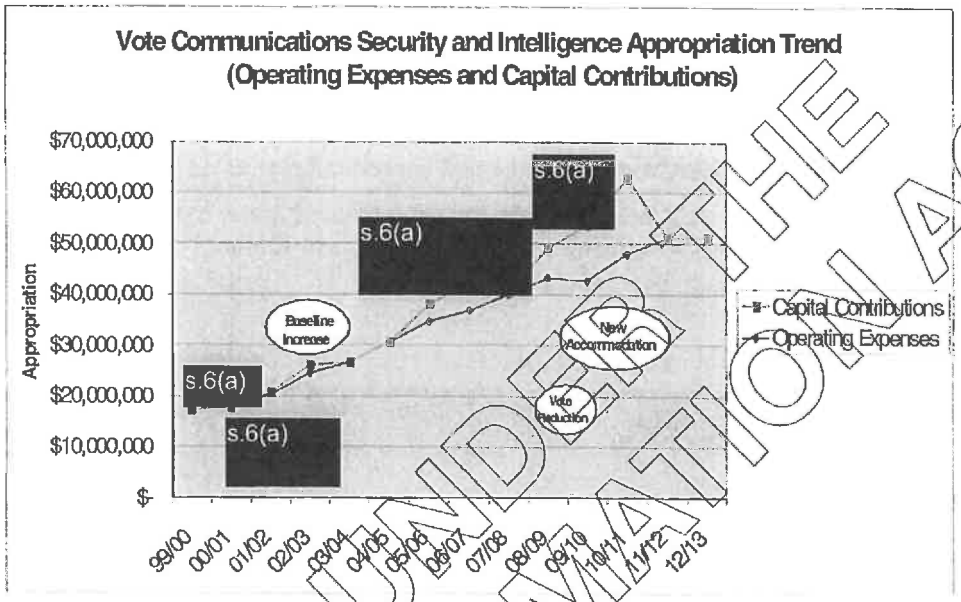
GCSB, NZSIS, EAB, DDIS, and NZDF Geospatial Intelligence Unit
Annual Appropriations/Budgets
(Operating Expenses)



3 During this review agencies were asked to look back over this period of growth and account for it. They see the funding increases broadly as having enabled a robust response to a major tempo/technology shifts:

- the ongoing response to 9/11
- s.6(a) [redacted]
- the rise of the Internet and the move to IP based networks, virtual private networks and wireless technology, and cyberspace activities to conduct both business and personal functions
- the growth and the pervasiveness of computer networks
- the converging of technologies and the speed and the emergence of new technologies
- the emergence of electronic attack via the Internet
- s.6(a) [redacted]
- a growing awareness for the need to have secure communications devices and effective IT security environments
- s.6(a) [redacted]
- the broadening of official information and the impact of various e-Government initiatives
- s.6(a) [redacted]

Government Communications Security Bureau



4 In the SIGINT environment, the funding has been applied to:

- s.6(a)
- development of a customer relations centre
- s.6(a)
- increased use of partnerships both in NZ and overseas
- s.6(a)
- greater use of s.6(a) to facilitate the distribution of SIGINT information and advice.

5 In the Information Assurance (IA) environment, the funding has enabled:

s.6(a) [redacted]

- increased demand for the provision of advice and assistance
- increased requirement to research and understand new technologies
- development of watch and warn for potential and actual cyber threats, research and analysis to assist mitigation against threats, and outreach to facilitate information exchanges and awareness (i.e. the Centre for Critical Infrastructure Protection (CCIP))
- updating of policy standards to meet the new and emerging technologies

s.6(a) [redacted]

6 Funding has also enabled:

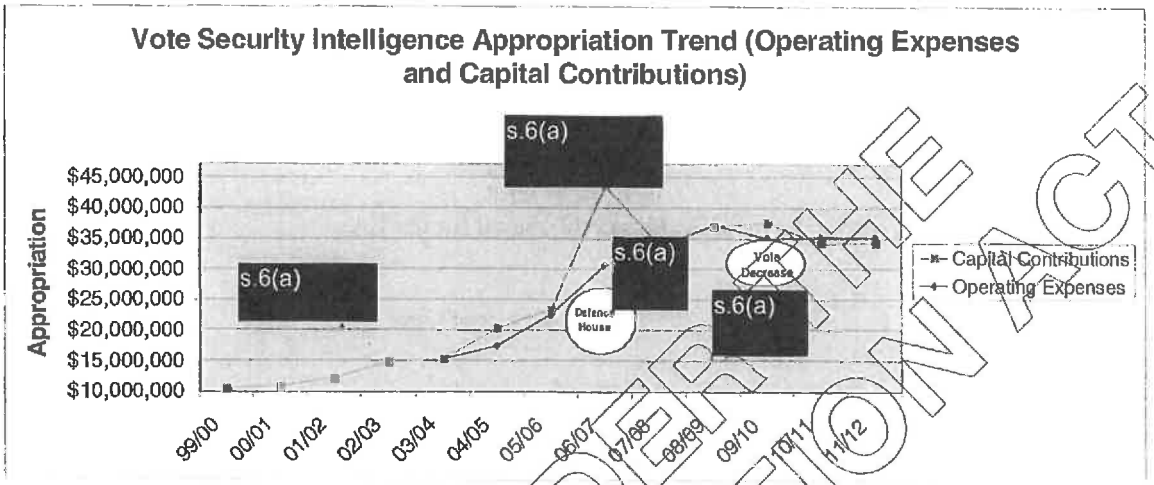
s.6(a) [redacted]

7 The need to develop cost-effective solutions for both SIGINT and IA activities for Information Technology and Communications and for the Corporate Services functions has led to:

s.6(a) [redacted]

- accommodation that will facilitate collaboration and team work, and assist in the recruitment and retention of staff.

New Zealand Security Intelligence Service



8 Funding has enabled:

s.6(a)

- Modernisation of infrastructure - such as the new accommodation in Defence House

s.6(a)

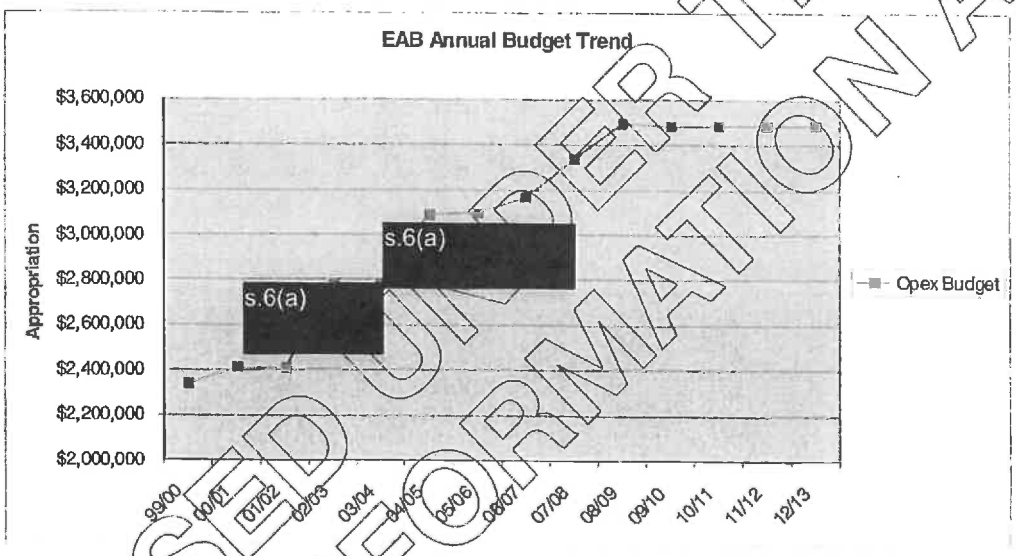
- Cost pressures - personnel costs including incentives to retain staff and the 2009/10 baseline reduction.

External Assessments Bureau (EAB)

9 Until the FY2000/01 the budget for the EAB was relatively static at about $2.3M (GST exclusive) but by FY2009/10 the budget had risen to $3.5M. The current planning baseline for FY2012/13 is $3.5M.

10 This increase has been caused mainly by the continuing 9/11 response, an increase in customer requirements and personnel cost pressures.

The graph below shows the trend in the annual budget for the EAB.

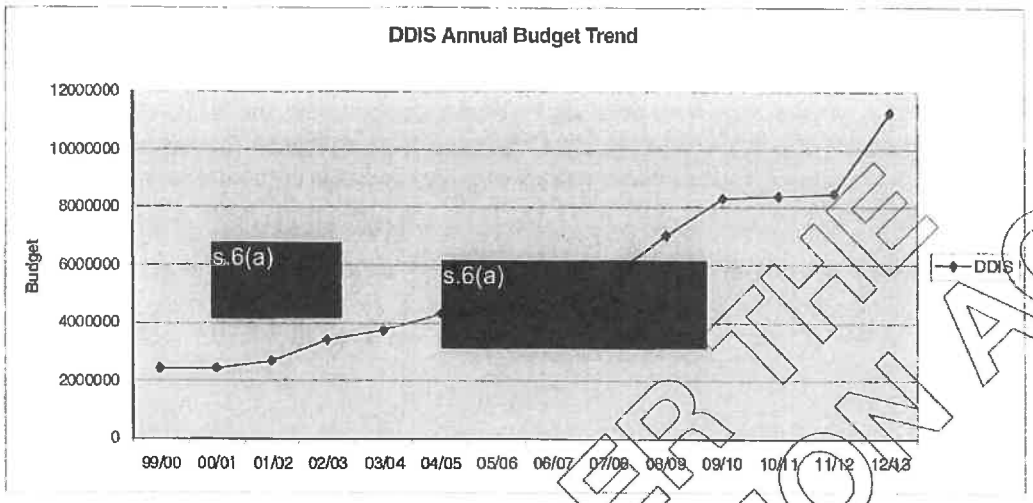


Directorate of Defence Intelligence and Security (DDIS)

11 Until the FY2000/01 the budget for DDIS was relatively static at about $2.4M (GST exclusive) but by FY2009/10 the budget had risen to $8.3M. The current planning baseline for FY2012/13 is $11.3M.

12 This increase has been caused mainly by the continuing 9/11 response and the implementation of the Intelligence Enhancement Programme.

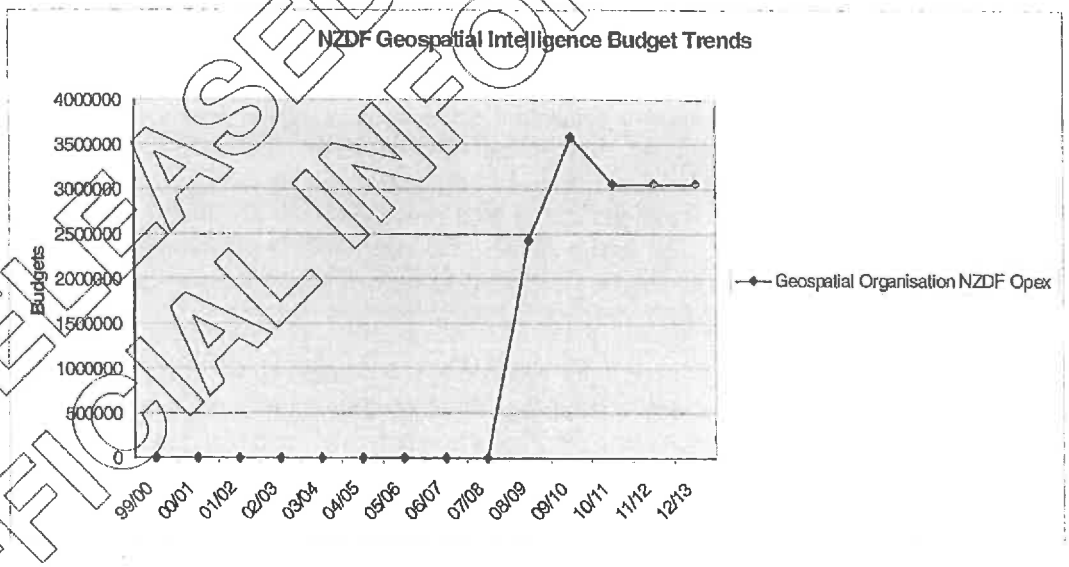
The graph below shows the trend in the annual budget for DDIS.



NZDF Geospatial Intelligence Unit

13 The NZDF Geospatial Intelligence Unit started in FY2008/09 with a budget of $2.4M. The budget for FY2009/10 is $3.6M and the planning budget for FY2012/13 is $3.1M.

The graph below shows the trend in the annual budget for the NZDF Geospatial Intelligence Unit.



Savings and Efficiencies; Corporate and Infrastructural Support Arrangements of GCSB, NZSIS and EAB

14 The budget outlook requires agencies to manage within current baselines and to fund themselves for growth where possible by repriorisations. For the NZIC collectively there is the prospect of some efficiency gains emerging from a planned approach to cross-agency shared services and related collaborations and alignments in corporate support delivery and purchase.

15 The Review accordingly probed the corporate and infrastructural support arrangements of the three intelligence agencies. Its purpose was to develop an understanding of the potential for greater collaboration and shared services to support agency and sector performance.

16 Due to the nature of the businesses, a full or partial integration of some services may not be possible or desirable. Particular agency outcomes, or specific agency powers, could impede opportunities. Careful thought will need to be given to preserving some distinctive values where these are important to domestic and external partners. Nonetheless, taking account of the security risks and optics, some aspects of in-house and standalone corporate functions and services could be better joined up to realise a community-wide good.

17 In the course of the review it became clear that for NZSIS in particular, the prospect of being required to find "back office" savings causes difficulties. This is because their agency is halfway through an ODESC approved internal remedial programme to modernise and strengthen those services. The aim, broadly, is to address the risks arising for the NZSIS front-line from failures in the administrative tail where it is providing services of the 'close operational support' kind.

18 To incentivise the intelligence agencies to explore opportunities, an 'efficiency dividend' is proposed for the NZIC. Agency heads and second tier managers would be required to develop plans for cross-agency service delivery in areas where savings are clearly achievable and the risks of compromise to frontline effectiveness are manageable. Pooled corporate and back-office functions and shared processing and distribution technologies should be characteristic of the future NZIC. Savings and/or reprioritisation targets for NZIC collectively would be set as a dividend to be realised at the end of a three year programme.

19 At the outset of the review, it had been intended to try to take a closer look at the 'factory' aspect of NZIC – the ways in which finished intelligence is actually assembled, across the agencies. However, to deconstruct the production systems, distinguishing between costs that are embodied in the work practices of skilled staff, and separating out the costs attributable to the plant and machinery they utilise, or the business processes and practices they follow, has not proved possible. Perhaps it is an approach better mandated to the agencies themselves; they have already, individually, taken some 'working smarter' steps of this kind in order to be able to cope with the volume and tempo pressures of the last few years. It should certainly be considered as part of the overall 'efficiency dividend' concept and the subject of best business practice interchanges both within the New Zealand community and with foreign partners.

20 A more limited approach had to be taken. However, it did prove possible to 'drill down' and test, with agencies, individually the prospectivity for savings/efficiencies in the following functions:

i. financial management systems
ii. human resource systems
iii. information technology
iv. knowledge management systems
v. security systems
vi. organisational management systems
vii. property/asset management systems.

21 From this work, sectors where it might be possible to move to a collective direction include:

i. financial management systems – an integrated FMIS might provide a common platform for accounts payable and receivable, general ledger, tax management and purchasing. Internal risk management audit services and processes maybe another possibility for some pooling arrangements.

ii. human resource management systems – payroll, recruitment and retention, performance management, HR administration and learning and development are all functions that are difficult to outsource given their sensitive nature. Once security concerns are accommodated an integrated HRMS between the agencies could be a possibility. Joined up recruitment processes (psychometric and referee checking) and career-pathing across the agencies may also be possible.

iii. IT systems and services – both GCSB and SIS maintain high quality in-house IT services as part of operational core capability. Each has security sensitivities about what it does and doesn't do in the use of operational technologies and both are subject to the constraints of the law. Nevertheless, there are a range of in-house IT activities, elements of which (management, administration, support and development) could be rationalised in a shared services 'shop'.

iv. s.6(a) [redacted]

v. security – given both the large agencies generally share the same precinct, which when combined with a co-located EAB (and perhaps DDIS) in the new 'Intelligence House' (new Pipitea Street building), may point to realisable efficiencies.

vi. organisational management systems – the GCSB's and NZSIS's audit committees have common external advisors which suggests the possibility for a single intelligence audit committee. Also, better aligned business planning, strategy and performance processes may also deliver common efficiencies.

vii. property/asset management – asset registers (aside from property) contain business enabling assets unique to NZSIS/GCSB and given the nature of agency accommodation it is difficult to see a reduced overall occupancy footprint in Wellington. There might be something at the margins that should be shared or used more widely which is best left to the agencies to identify. In a broadened new Intelligence Community, given many operations occur outside of Wellington, prospects for asset sharing might also be explored especially for NZSIS as it seeks closer engagement with the law enforcement and border sectors.

viii. s.6(a) [redacted]

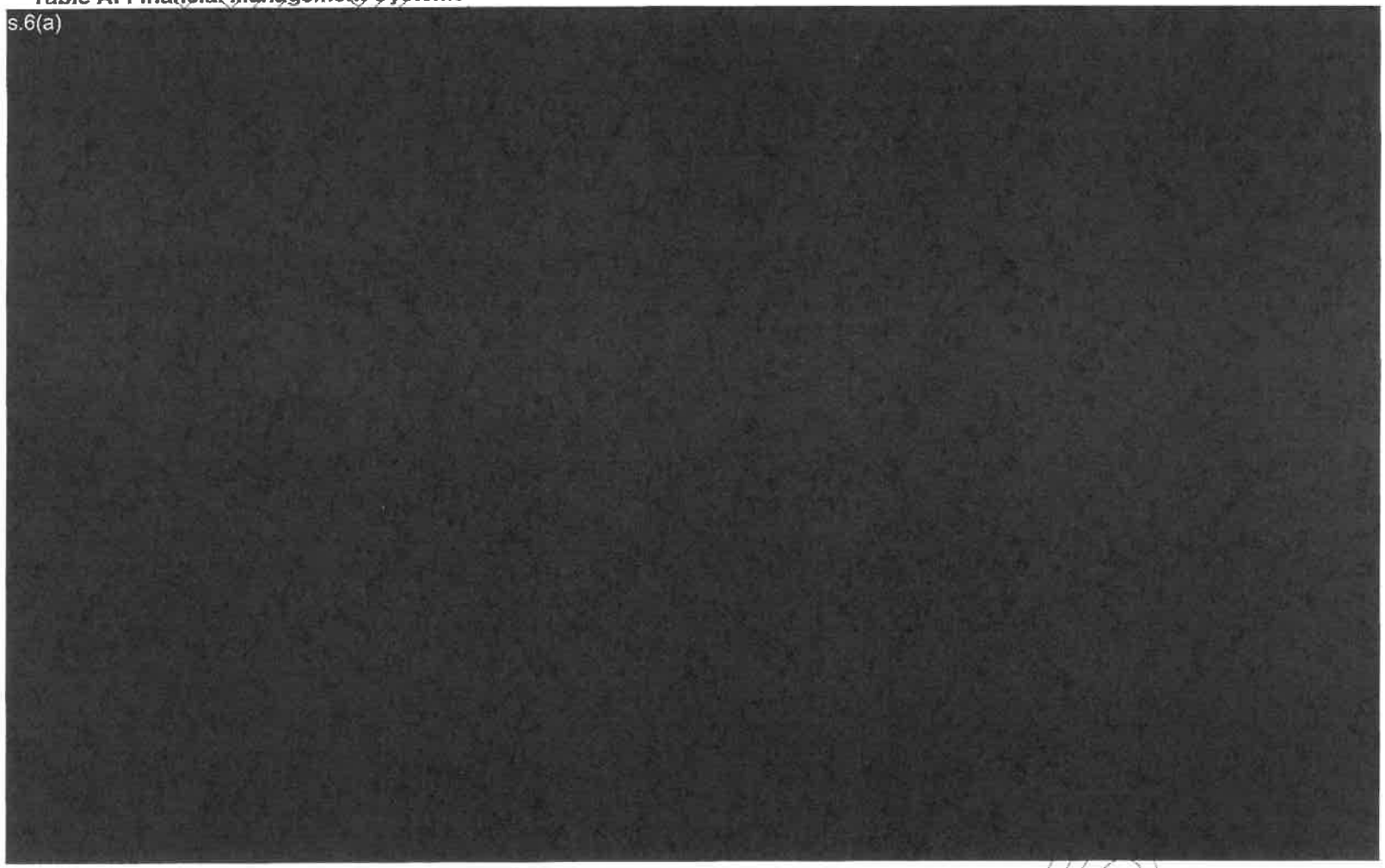
22 The Review was provided with information identifying the corporate hardware and processes of each of the agencies which support the systems referred to below (see table A). The viability of agencies to share or shift corporate functions can be tested from this information base. Generally, some functions and activities undertaken in each agency are very thin and the consolidation of critical mass, where appropriate, could support organisational and sector resilience. Staff numbers assigned to each agency's corporate activities (i.e. finance or HR) is a factor of small siloed organisations requiring a broad reach. The potential for economies and staff savings may also be realised (see table H) through further research.

23 The size of the agencies and relatively low volume of transactional processes does not suggest staff savings will be achieved through pooled or shared services. However, at the very least, while economic benefits may be very modest a stronger collaboration culture is expected to be forged.

24 Annual plans incorporating a two year review programme analysing the feasibility of opportunities listed in paragraph 20 above need to be developed beginning with the two primary intelligence agencies and extending then to EAB in regard to the assessments cluster, but ultimately spanning the wider contemporary community. The programme might be particularly informed by scheduled replacements or upgrades to infrastructure or internal agency reviews. The agencies will be inspired by the programme's overall purpose which is to support agency responsiveness, sector coherence and service delivery and hence should make every effort to achieve greater efficiency, economy and efficiency.

Table A: Financial Management Systems

s.6(a)



Cost Efficiency Opportunities

Efficiencies could be gained through a single:

(a) accounts payable and payment system (except sensitive)
(b) accounts receivable (debtors) system
(c) purchasing system

It may also be possible to create an integrated FMIS system with GCSB and NZSIS set up as separate 'companies'. Careful thought will need to be given to the sensitivity of some transactions, agency operations and staff details to avoid security being compromised. Access control compartmentalisation may be an option which will necessitate business rules as to which agency has authority and oversight of the entire FMIS system.

The finance function also provides manager support. The number and locations of managers and functions drive the size and location of the advisor and support element of the finance function.

Table B: Human Resource Systems

s.6(a)

[redacted]

Cost Efficiency Opportunities

It is possible to develop an integrated HRMIS system that could accommodate GCSB and NZSIS as separate companies. Compartmentalising through access controls to preserve security (via encryption) could be an option and, if required, highly sensitive matters (e.g. names and location of operational NZSIS & GCSB staff) could be maintained on a standalone system. Oversight (host employer) of the whole HRMIS system would require consideration.

Synergies are possible in joined up recruitment and career-pathing across organisations to increase opportunities in relatively flat-structured agencies. Efficiencies might arise via bulk purchasing rates for recruitment processes s.6(a) and referee checking s.6(a)

Table C: Information Technology Systems

s.6(a)

[redacted]

Cost Efficiency Opportunities

Initial probing suggests a single IT shop may be a viable proposition. At the very least, greater synergies could be achieved through shared corporate IT services and personnel.

Efficiencies/savings through leveraging enterprise agreement structures to reduce licensing costs (via greater number of users) may also present opportunities.

Table D: Knowledge Management Systems

s.6(a)

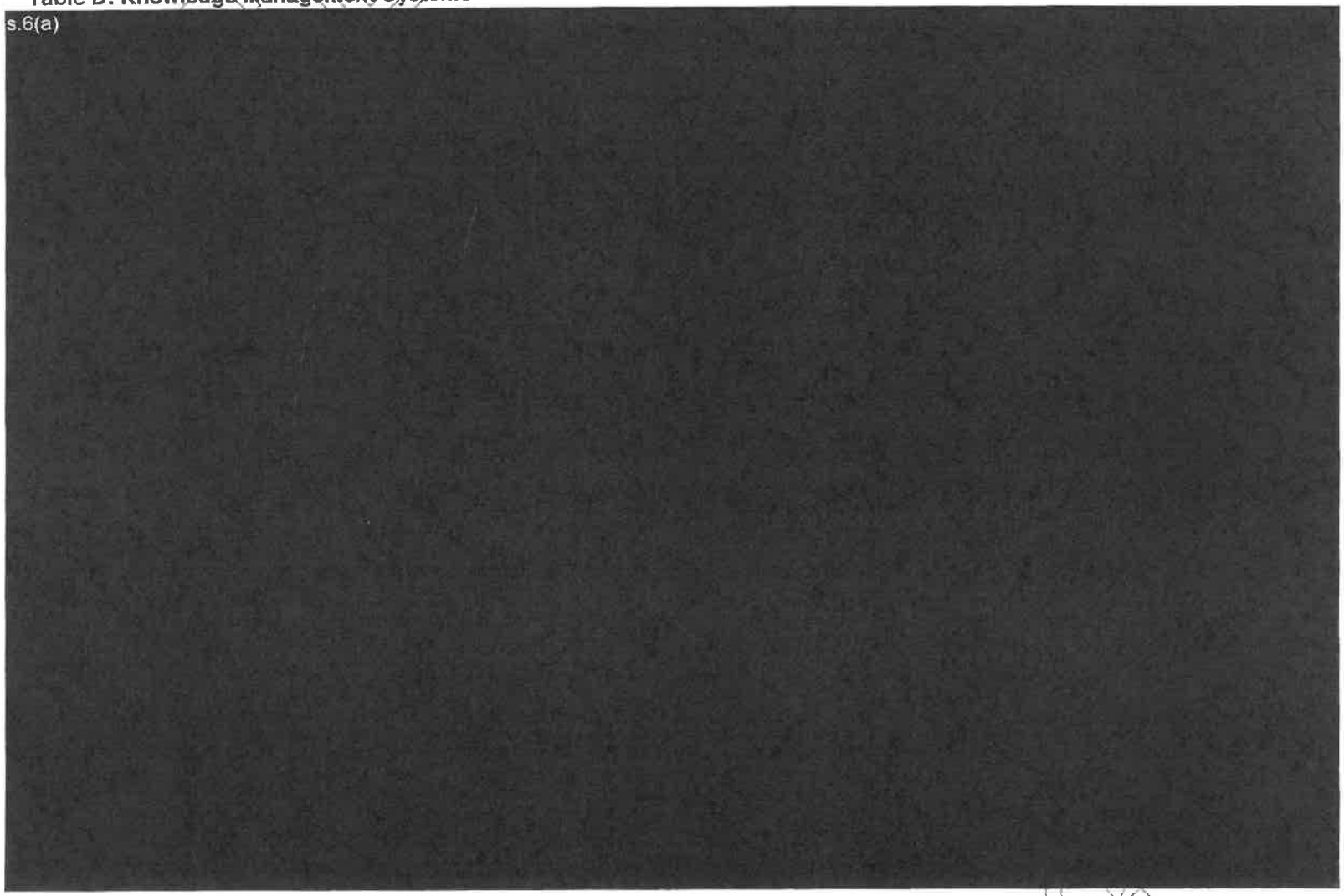


Table E: Security Systems

s.6(a)

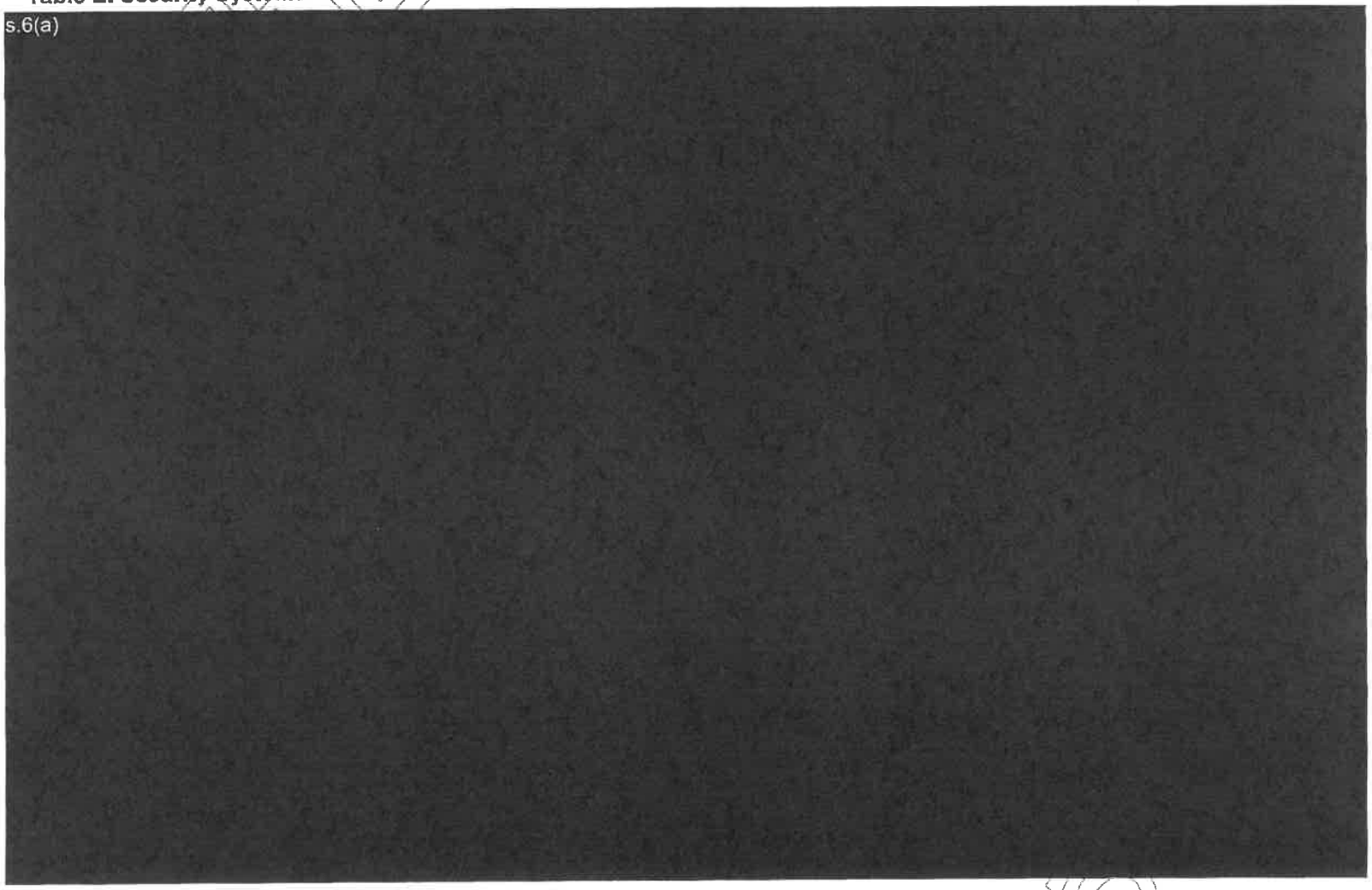


Table F: Organisational Management Systems (OMS)

s.6(a)

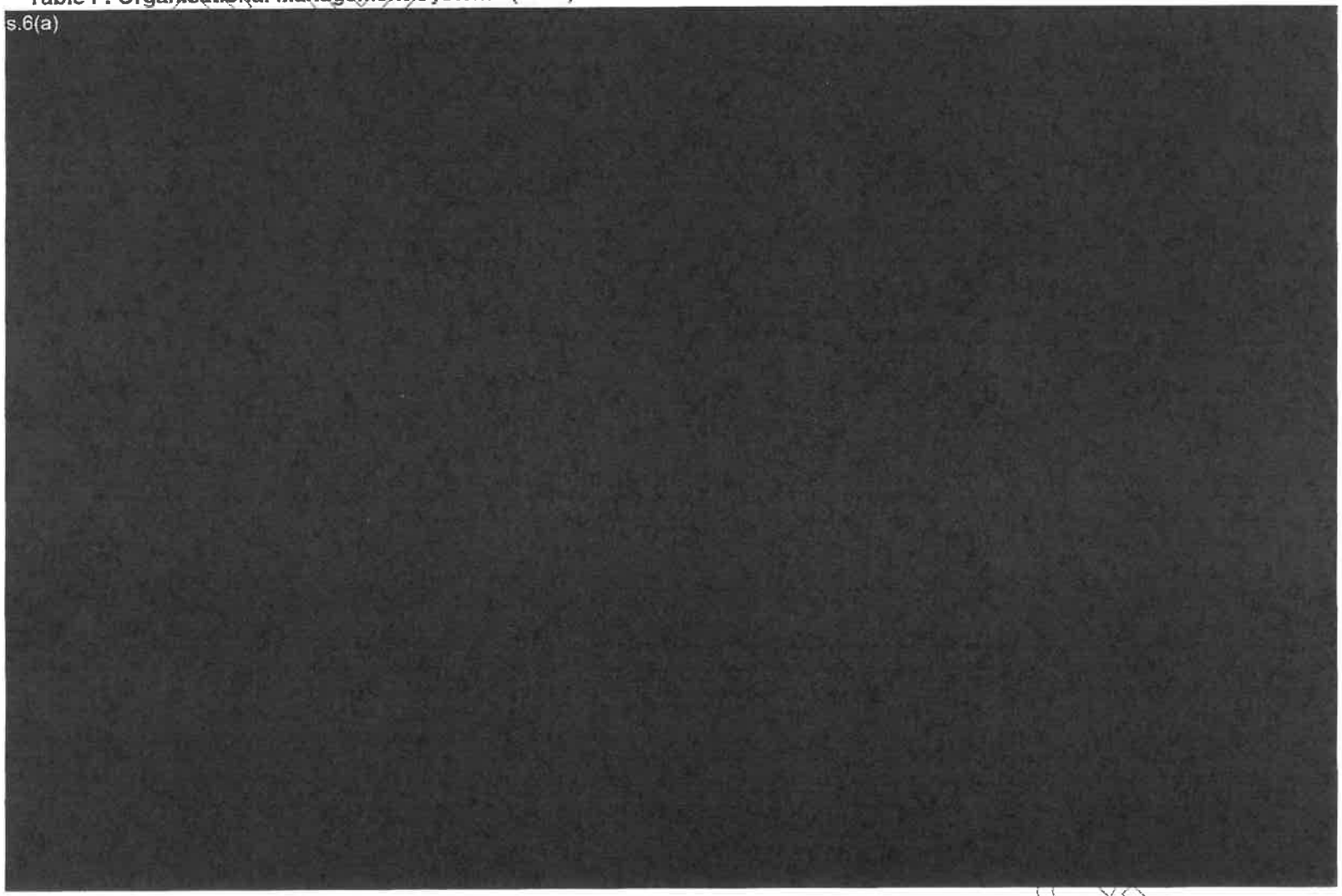


Table G: Property/Asset Management

s.6(a)

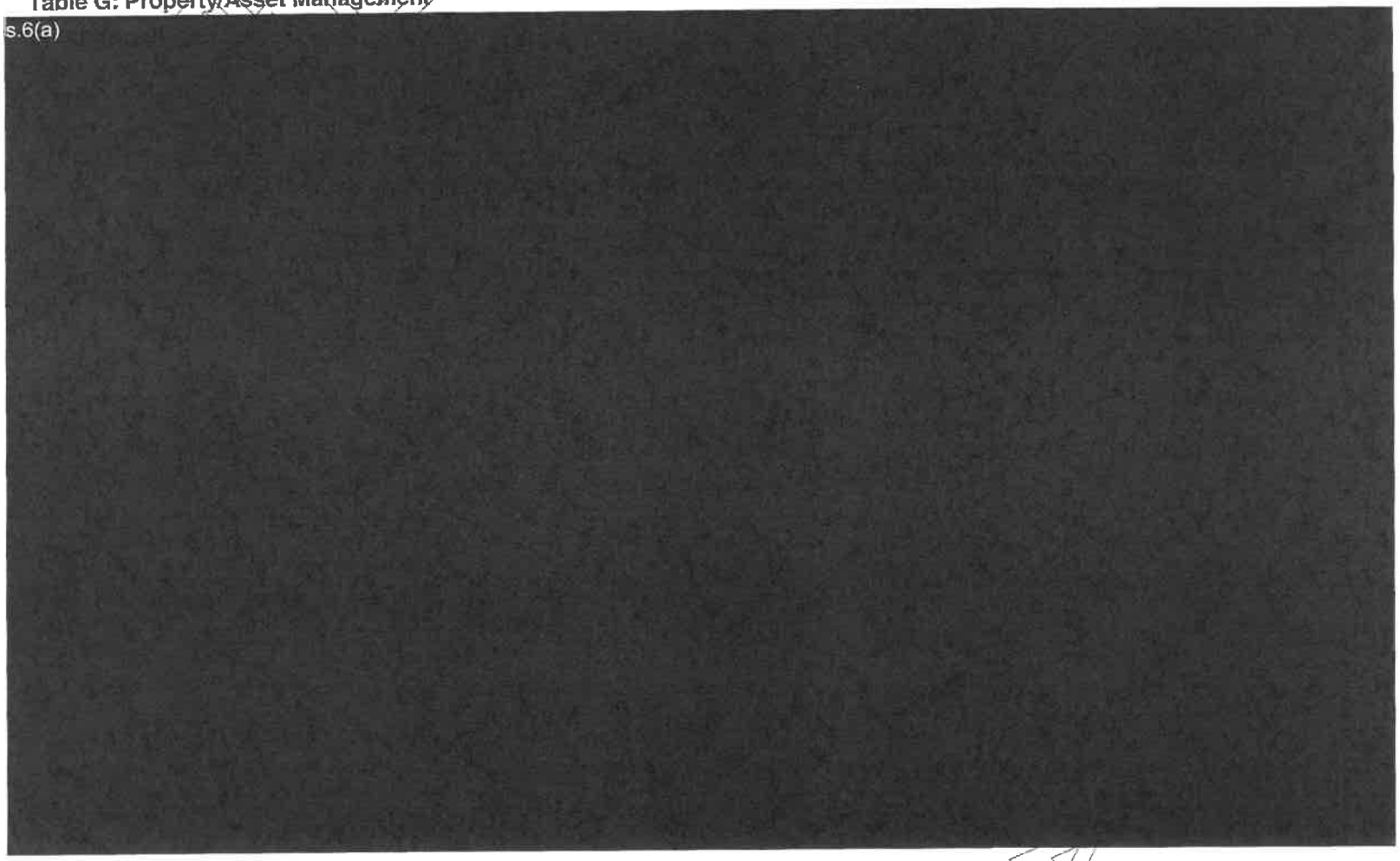
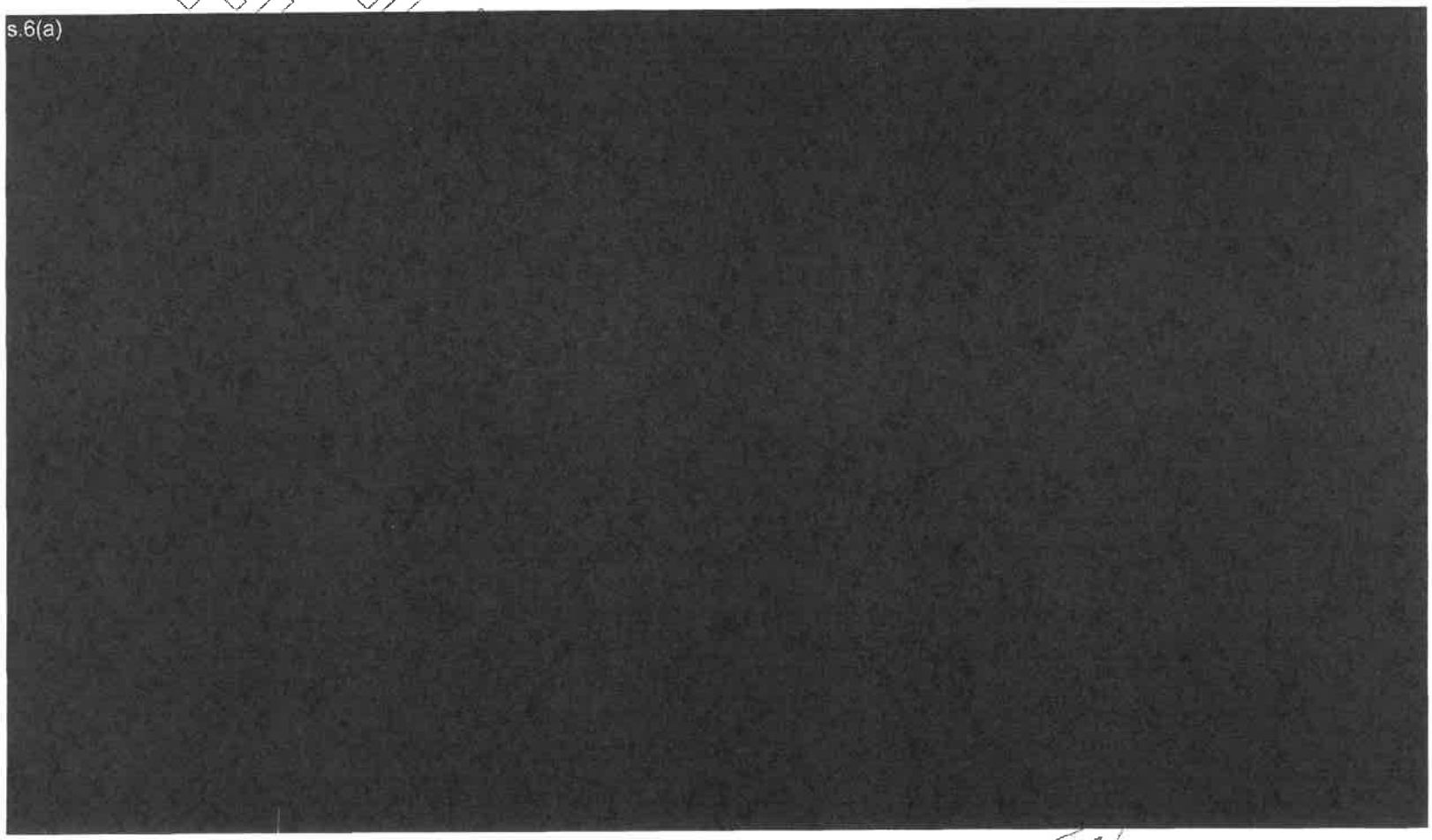
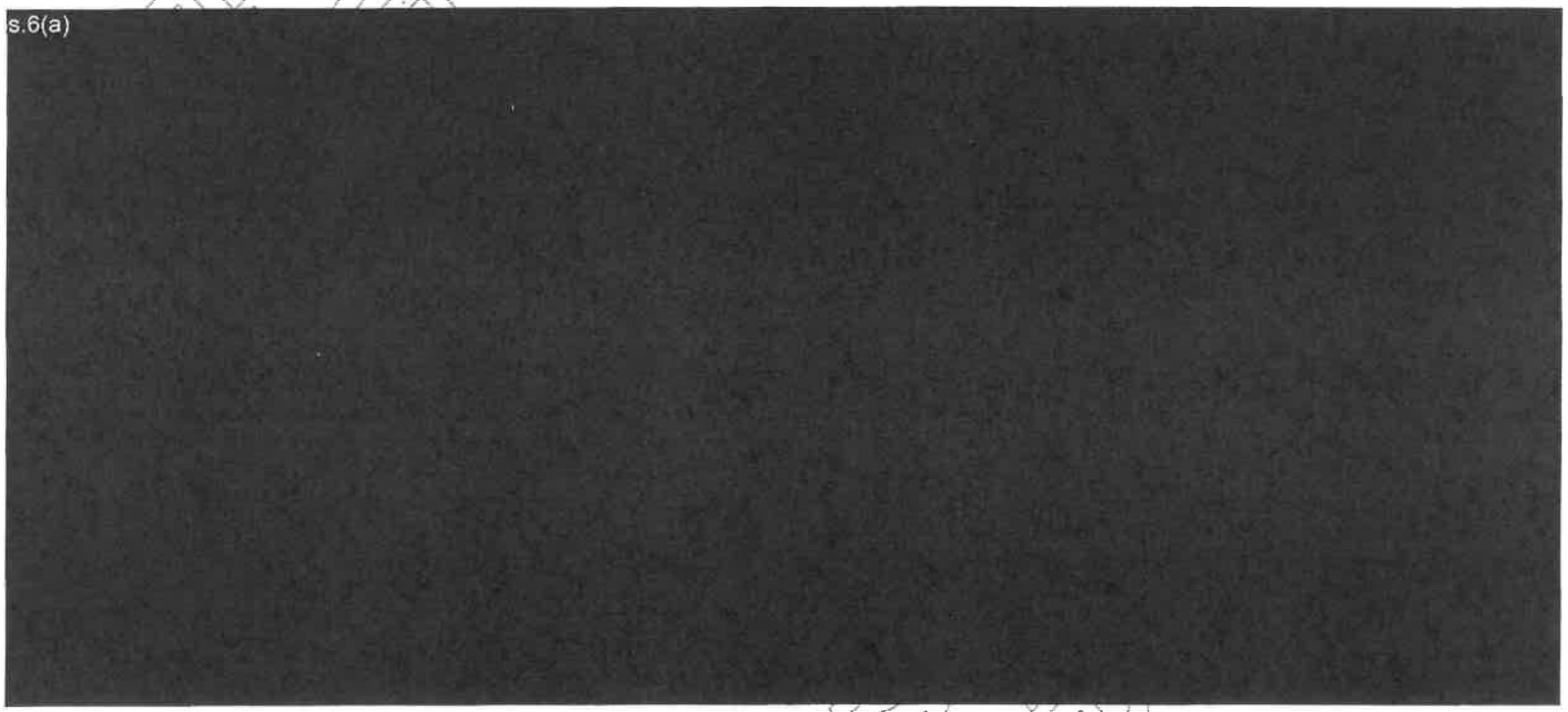


Table H: Corporate Office - GCSB, NZSIS and EAB

s.6(a)



s.6(a)



Annex 5: Governance of NZIC, Accountability and Authorising Regime

1 National security coordination and oversight of the intelligence community have always been seen as the province of the Prime Minister for good political and constitutional reasons. Until relatively recently Executive responsibilities for intelligence were not shared much with other Ministers, and the role of Cabinet has been quite limited. Appropriate institutional forms to support the PM in carrying out these duties did emerge but rather slowly. For many years it was in the very restricted format of the Defence Council that the interface was recognised. The original (two person) Domestic and External Security Secretariat (set up after Cyclone Bola and the first Fiji coup) had no institutional moorings until the formal creation of the DPMC in 1990 when it, and EAB, were incorporated as business units. At that time two ad-hoc Cabinet Committees were established: one for domestic/external security coordination and the other, with a more restricted membership, for 'intelligence and security'. In 1994, the position of Intelligence Coordinator was established in DPMC and occupied by the recently retired Director of NZSIS. This position was seen as critical to the development of a more explicit targets and requirements process, modelled on the British Joint Intelligence Committee (JIC) and based on more conscious responsiveness to the needs of policy agencies as customers. There were also significant 'transparency developments', changes to Parliamentary oversight arrangements and the creation of an Inspector-General to be an independent monitor of the use of statutory powers. GCSB became a declared state agency via its own legislation. Coinciding with this development, Sir Geoffrey Palmer gave a first ever overview of the then contemporary security and intelligence system. In an official publication ("Securing Our Nation's Safety") he offered reassurance about the robustness of political and parliamentary accountability, as well as of the executive governance of the system. Describing the functional configuration of the NZIC, in a collective sense, and role allocation within it, he focused particularly on the role of the ODESC, the principal vehicle for the delivery of "policy advice, decision support and review capability" to the PM and Cabinet. He noted explicitly that it was the ODESC membership of CEOs who collectively held systemic responsibility for administering "the overall intelligence activities of the government"[4].

2 In 2003 the Auditor-General reviewed the post 9/11 funding of the NZIC, and related agencies, in terms of a 'homeland security' response to the new terrorism. Responding to that report, in 2005, DPMC formally promulgated Cabinet approved guidelines ("TOR") for ODESC itself, in respect of crisis management, security preparedness and "intelligence oversight". This document, which may have had minor updating, remains the 'charter' for the NZIC: the principal descriptor of its governance and authorising architecture. It lays down a single Cabinet Committee (DESC) at the peak whose intelligence mandate is to "address oversight, organisation and priorities issues" as and when directed to do so by the Prime Minister. The specified role of the ODESC intelligence grouping of senior officials "ODESC(I)" is for foreign intelligence and the scope of responsibilities is defined as "national assessments coordination monitoring review, external relations and budget scrutiny". The agency heads are all full members of ODESC(I). The Intelligence Coordinator is not; he is "responsible to" the Committee but reports through the Director DESG, and has attendance rights but is not the secretary to the Committee.

[4] See Palmer report organogram

3 These governance arrangements are all reflective of both the "need-to-know" constraint and an underlying instinct to be wary of over-centralisation with attendant risks of blurring or displacing the direct legal and other output delivery accountabilities of the individual agencies. NZIC generally, it has been thought, should operate with a relatively weak centre. The 2005 TOR speaks of the role of DPMC/DESG as being to facilitate whole-of-government behaviours and coordinate between the various agencies delivering foreign intelligence outputs. Aside from the careful delineation of the Coordinator's status, there is relatively little in the 2005 TOR about the allocation of roles within and between the agencies that make up the community. Confidentiality may well have been an inhibiting factor (especially with regard to sensitive collection projects or activities) and it is possible that the job descriptions and performance agreements of individuals (which I have not asked to see) contain relevant material. But relative to the "foundation documents" of other partner jurisdictions, the NZIC charter, at least in terms of individual responsibilities and accountabilities for system-level performance and behaviours is much less fully articulated.

4 Being largely Wellington based, and given above average levels of collegiality amongst long serving senior management cadres, the NZIC, as a largely foreign intelligence construct, probably has had less need than overseas counterparts, to go beyond the 2005 TOR in defining itself systemically. It has been characterised by informal networking and by a habit of professional conversation which only required light facilitation by DESG. Certainly NZIC has been able to avoid the dangers of excessive siloisation and over-compartmentalisation that can develop between standalone intelligence agencies which see their methods and their product as deeply specialised. In other jurisdictions these are defects that are considered to have caused intelligence failures: available knowledge was lost in the cracks, misdirected or even distorted and that opened the way to decisions of state with serious public welfare or international relations consequences being either not made at all or badly made. But when one considers the real breadth of the contemporary national security agenda with its greater complexity, and the rising demand pressures on NZIC it is hard to say "leave well alone", and continue to rely on innate collegiality or the limited coordination practices and centralised governance that have been the historic norm. The almost certain need for a lengthy period of fiscal restraint simply exacerbates these risks and exposes the danger that the NZIC will be unable to sustain its levels of performance: the quality of its service delivery or its operational soundness or its intellectual acuteness could erode, by degree. It could fail to fully utilise the materials it now has access to. Ministers are entitled to be assured that NZIC's structures are future proofed, that its overall management of its inputs to national security will be sustainable and will meet acceptable standards.

5 In practice the post 1990 structure has done the job pretty well. It enables the integration of intelligence into operations notably, in the foreign relations space, the exposure of policy risk at the cross-agency level and wider scoping of options for advice to Ministers. And it has been very successful in planning for and coordinating actual immediate emergency response, especially to complex events with onshore/offshore dimensions.

6 But, viewed from the systemic perspective of integrating intelligence with national security across a wider set of actors, and of sustaining performance and capability at a time of some risk (fiscal and otherwise), ODESC(I) as it stands does not have the right mandate or membership. To be able to act in the governance mode would require a differently composed group - ODESC(G) with a clear mandate. Still chaired by the CEO of DPMC, it would include the other two central agency CEOs as standing members.

There should be some representation, rotational from the wider NZIC, perhaps a CE each from agencies which principally deal in foreign and "homeland" intelligence. Other ODESC(I) CEs should participate as required by the agenda. Heads of the intelligence agencies would remain standing members of ODESC(I) but their participation in ODESC(G) would be agenda-driven and avoiding conflicted roles. They should not 'sit in judgement' on each other's budgets or performance. The Intelligence Coordinator and the DESG Coordinator should both normally attend. They would be held accountable for their coordination performance when ODESC(G) reports to the PM and Cabinet on the overall wellbeing of the national security system and NZIC's support of it.

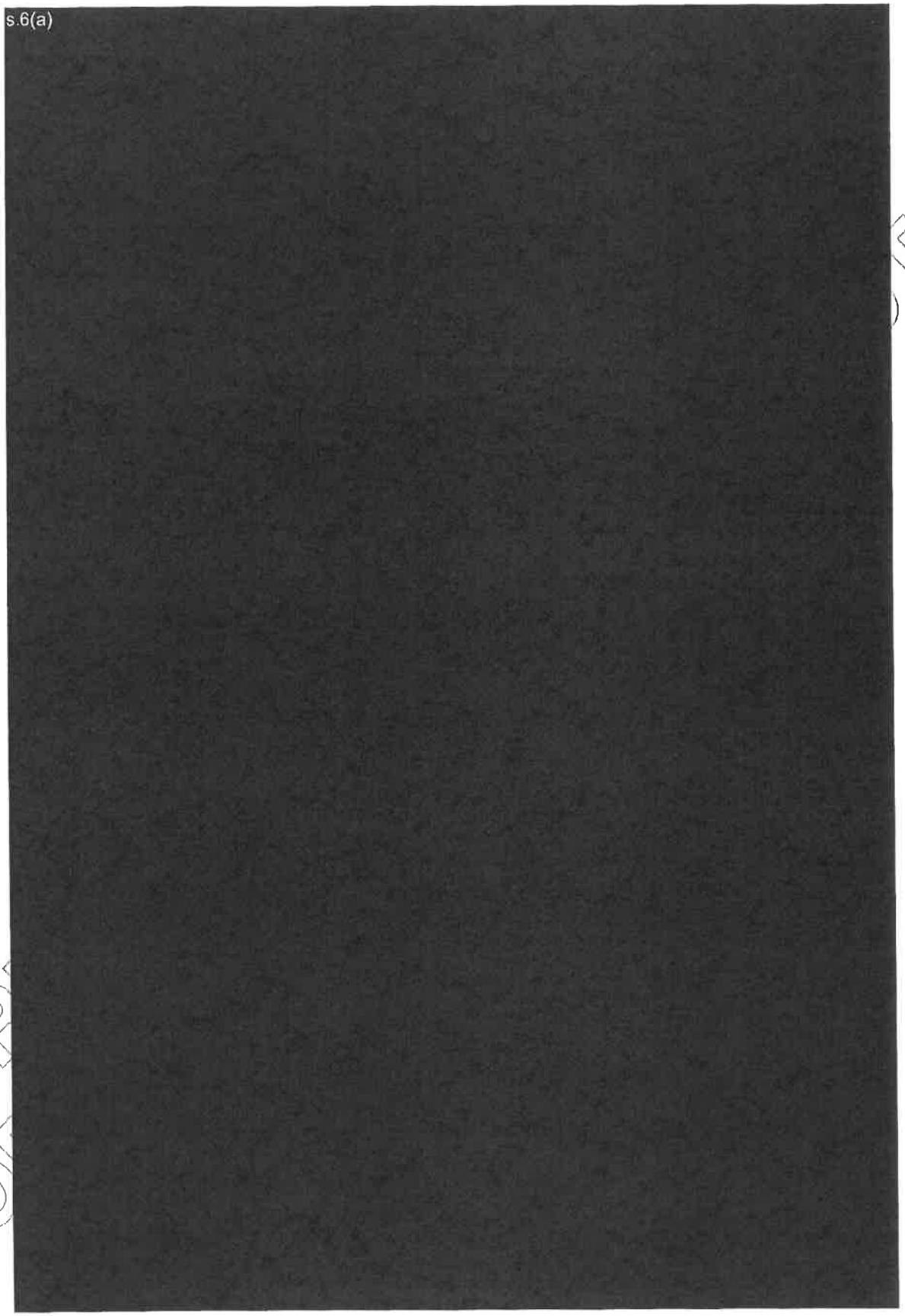
Annex 6: Allied Partnerships; Governance Changes and Relationship Management

1 In the aftermath of 9/11 and the Iraq war, the 5-Eyes nations either came around to, or were required politically (in response to intelligence failure accusations and findings) to make changes to their accountability and governance arrangements for national intelligence coordination at policy and operational levels. Whilst it has not been possible in this review to fully examine the detail or real extent of these changes (some are still unfolding) it can be said that our close partners have all attempted to step up interagency coordination of outputs, and to revisit the mandate and scope-of-role for the key actors in their systems i.e. those directly responsible for driving a contemporary national intelligence community that responds effectively to national security policy priorities. There has not been any major machinery-of-government change of the structural kind (e.g. a merger) to their agencies in these jurisdictions. But in their approaches to budget and resourcing, partner governments appear to have seen the need for a better overview at aggregate level, and the British innovation of a "single intelligence" "envelope" or "account" is being watched with interest. Value for money and where best to invest in extra capability are particularly pressing considerations, not least because the costs and lead times for new technology have to be managed against a sense of urgency about gaps (the "unknown unknowns"). The need to be able to use existing resources more flexibly heightens generic concerns about resource stickiness, (operator capture, budget hoarding, etc) in intelligence structures, given the logic that they operate as standalone businesses and given that they must compartmentalise information about outputs for security reasons. Governments are more deeply averse to the consequences of being caught with too many eggs in the wrong baskets.

2 Other factors influencing the mood for change have included a commonly-perceived need to revisit and broaden the standard definitions of "national security" to better recognise the permeability of the contemporary risk boundaries between foreign and domestic/homeland. And there is a concern to emphasise the importance of systems that enable the vocational branches of intelligence as a profession to interact more freely across organisational structures and disciplines to a wider mutually-understood set of bottom-line risks and targets. In short to lift the "professional conversation" out of any silos, and increase its frequency and push it into new areas of common purpose.

3 s.6(a) [redacted]

s.6(a)



4 s.6(a) [redacted]

5 s.6(a) [redacted]

6 s.6(a) [redacted]

s.6(a) [redacted]

s.6(a)

7

s.6(a)

8 The common theme in the reviews and re-engineering done by 5-Eyes counterparts is a strengthening of coordination machinery and of governance arrangements by changes which:

- more clearly define the intelligence community in terms of membership and/or status
- give clearer ownership for the prioritising of requirements and tasking
- locate intelligence within a wider national security policy context
- tighten the coordination machinery by designating and empowering responsible central actor/s
- (to varying degrees) centrally control budget and resource flows.

s.6(a) [redacted]

International Partnerships; Relationship Management

9 s.6(a) [redacted]

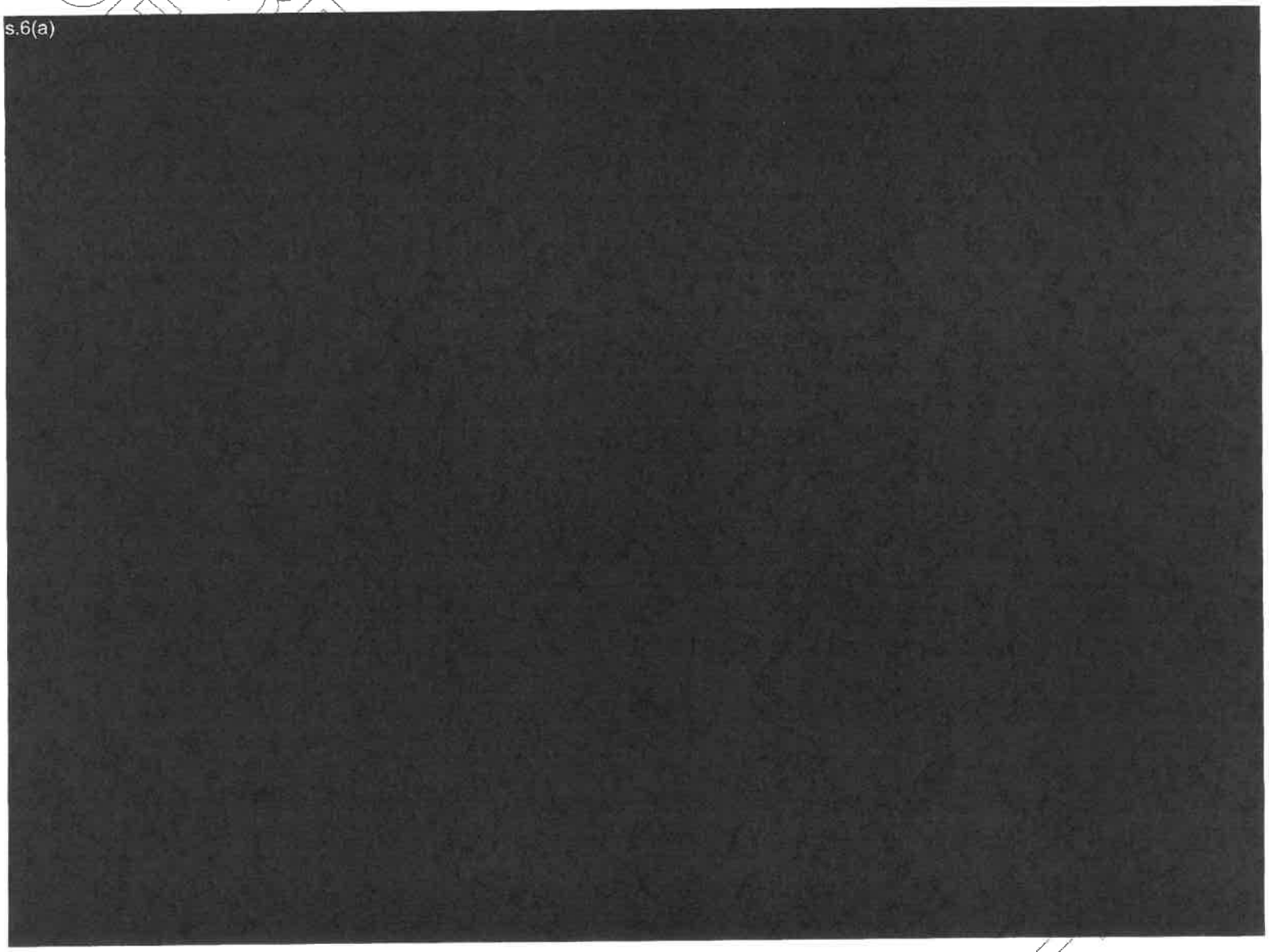
10

s.6(a)

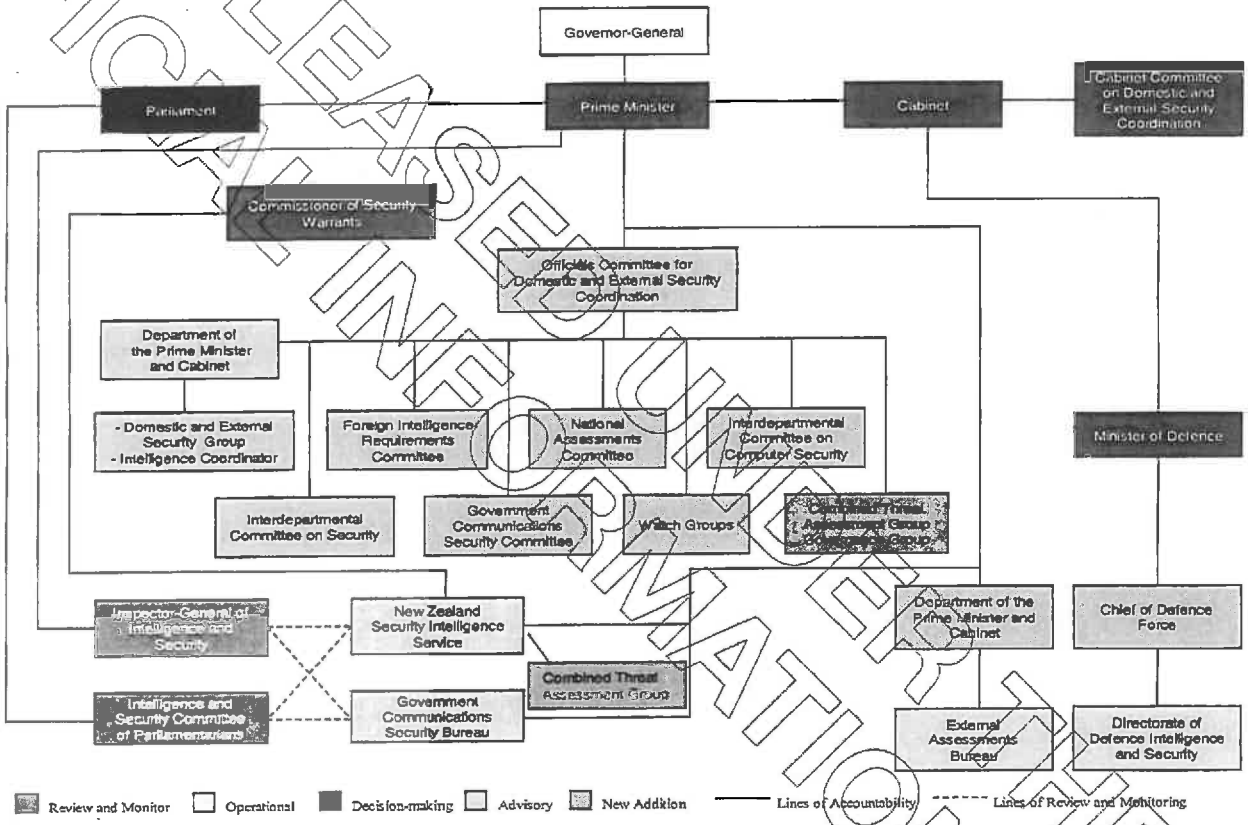
[redacted]

11 More importantly the question of coherence needs revisiting. In other jurisdictions, the Coordinator has been given seniority partly in order to be able to represent at senior officials' level a total grasp of the national intelligence effort to partner governments. In our case, whilst the PM is the point of authorisation for the content of offshore partnership activities and engagements of NZSIS/GCSB/EAB, there is no CE with such an overview, let alone one that takes in the intelligence dimensions of the new homeland security diplomacy. The CEO of DPMC may be best placed in our system through chairing ODESC and by proximity to the PM to be the single voice of NZIC when such a voice is needed. This needs to be made explicit and should mean that he, not agency heads, is the ultimate point of coordination for coherent NZIC messaging to partner governments.

s.6(a)

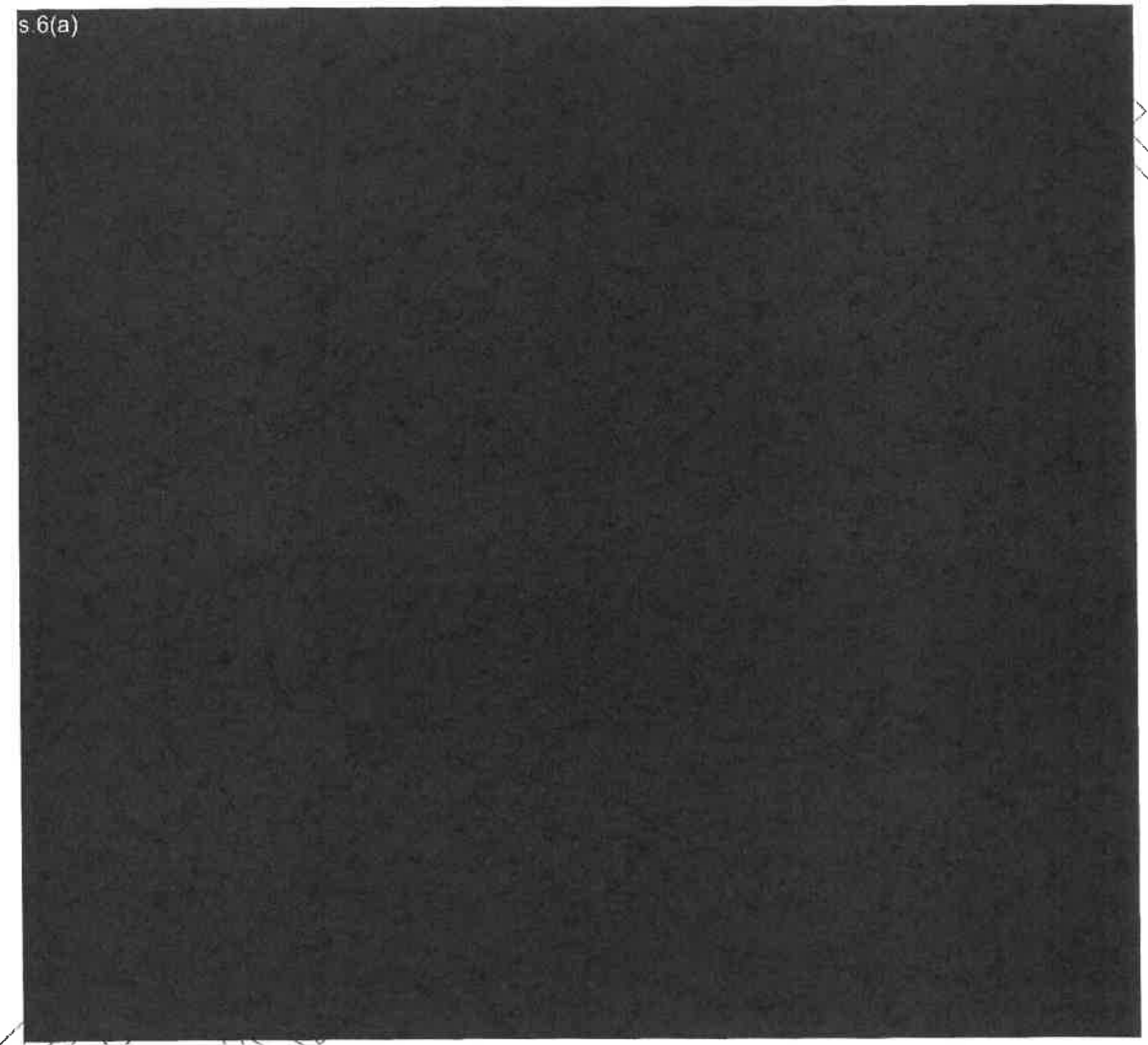


6



[6] Diagram, as amended in prescript, is taken from the DPMC/Sir Geoffrey Palmer publication "Securing Our Nation's Safety - How New Zealand Manages its Security and Intelligence Agencies" issued in December 2000.

Annex 7: The Intra-Community Conversation: NZIC Communication Habits



Managerial conversations (i.e. Head of Agencies meetings) or institutionalised meetings

16 Aside from monthly ODESC meetings, the Directors of EAB, GCSB and NZSIS have little formal contact with each other except on an issues basis. Bilaterals occur 'as-required' and communication may occur via secure telephone. Formal meetings are scheduled irregularly between the agency heads who often 'catch up' immediately after ODESC meetings.

17 Occasionally, agency heads support each other's overseas delegations directly or by alternating hosting dinner/lunch hospitality arrangements for overseas guests. Until recently, a semi-regular (bi-monthly) Heads of Agencies working lunch occurred between core agencies heads (NZSIS, GCSB, EAB, DDIS and DESG). The purpose was

to share issues and perspectives. These have however, have lapsed due to busyness of agency heads (the last meeting occurred in late 2008).

18 Generally, the 'sector' is not characterised by a framework for institutional meetings or managerial conversations and issues-based bilaterals tend to be the primary mechanisms for communications between agency heads.

19 A reinstated schedule of Heads of Agencies meetings focussed by an agenda that goes beyond issues-based bilaterals to sector outcomes focus, would potentially accelerate joint-agency work programmes and strengthen overall sector effectiveness. Significant performance agenda items could be targeted in a cyclical sense and might include:

- linking government priorities with a sector vision and strategy to achieve outcomes for stakeholders
- translating strategy into coordinated and joint agency planning (including SOIs and budget bids)
- adjusting organisational structures and policies to respond to sector needs
- sector management and coordination of infrastructural assets
- engaging, aligning and enthusing traditional and contemporary partners to work together as a team to deliver policy, strategy and services
- identifying the relationships that most significantly impact on its achievement of outcomes
- actively seeking the views of key stakeholders to inform decisions and relation management activity
- developing a sound knowledge base of the coordinated activities and relationships which are providing effectiveness and efficiency gains.

20 Membership of the Heads of Agencies should be reviewed with a view to incorporating new standing or occasional attendees.

Interagency conversations

21 Communication at the second tier level of the intelligence agencies and below is conducted informally.

22 Communication is also influenced by the foreign intelligence collection Requirements which has been relatively passive. Therefore communications between collectors and analysts has generally been underpinned by personal relationships targeted to the New Zealand collection in a specific portfolio area. Where significant material is provided through liaison means interagency communications tend to be much less.

23 There does not appear to be any regular informal gathering of the senior management responsible for the operational support and corporate administration functions of agencies. If the 'efficiency dividend' process is to be a success, some such 'practitioners group' will be needed, probably with central agency participation at an appropriate level and perhaps chaired by the Intelligence Coordinator.

Annex 8: Performance and Capability: Agency Self Assessments

1 Central agency knowledge of organisational management platforms of the intelligence agencies is, for a variety of reasons, not extensive. Aside from occasional Auditor-General reports, occasional briefings to ODESC, annual budget bids and some other limited high level human resource data, generally the administrative, management and operational capability of the intelligence agencies is not visible.

2 To supplement central agency knowledge, the Review commissioned the three intelligence Directors to undertake a self analysis of agency services. The assessment focussed on the delivery to government priorities, delivery of core business as well as organisational management dimensions on four quadrants, including:

- leadership, direction and delivery
- relationships and governance
- people development
- financial and resource management.

3 A diagnostic instrument, (the Performance Improvement Framework (PIF)), was used for this exercise (see figure 1). The PIF provides a relatively high level overview of departmental performance and identifies actions necessary to improve performance. For the purposes of this review, the PIF was used to create a baseline of standard information. It should be noted the PIF is still being evaluated and has not yet been formally adopted as a diagnostic tool for central agency standard use.

4 It should also be noted that EAB's PIF remains in draft as EAB is a business unit of a Department of Prime Minister and Cabinet and not a department per se. Secondly, the self assessments were not themselves analysed or tested by a 'lead assessor' as contemplated in a formal PIF process. However, they do offer interesting departmental and 'sector' perspectives (collated in figures 2 and 3) which inform this Review.

5 Both the larger intelligence agencies report similar challenges. For instance, both GCSB and NZSIS identify an absence of overall outcome and priority setting for the sector leaving individual agencies to make their own determinations. Similarly, both agencies claim to be under resourced. Finally, they were united in the views of maintaining NZ's place in the 5-Eyes community.

6 All three intelligence agencies indicate they are delivering to Government priorities and on core business. In the nine areas the agencies have defined as Government priorities they report that, in all but one area, they are maintaining or improving performance. Against the trend, GCSB reports its development of an Information Assurance capability especially in computer network defence is deteriorating.

7 As well, both GCSB and NZSIS report performance maintenance or performance improvement occurring in the Service Quality and Trust dimensions. EAB indicates it does not have any data to inform such an assessment.

8 In terms of organisational management, which determines how well the agency is positioned to deliver currently and in the future, the picture is mixed.

9 On a positive note:

- all three agencies advise they are well placed in the Relationships and Governance quadrant – particularly in engaging with Ministers
- they also have confidence in the Leadership, Direction and Delivery quadrant.

10 While agencies did not report any areas of serious concern what can be discerned is:

- there are only two of 13 areas where agencies indicate strength: NZSIS in regard to vision, strategy and purpose and EAB in regard to setting and managing performance expectations
- all three agencies agree that leadership and workplace development (in the People Development quadrant) is a development area
- the Financial and Resource Management quadrant is identified by all three agencies as the quadrant requiring more development work (especially managing assets, financial management, audit and risk management).

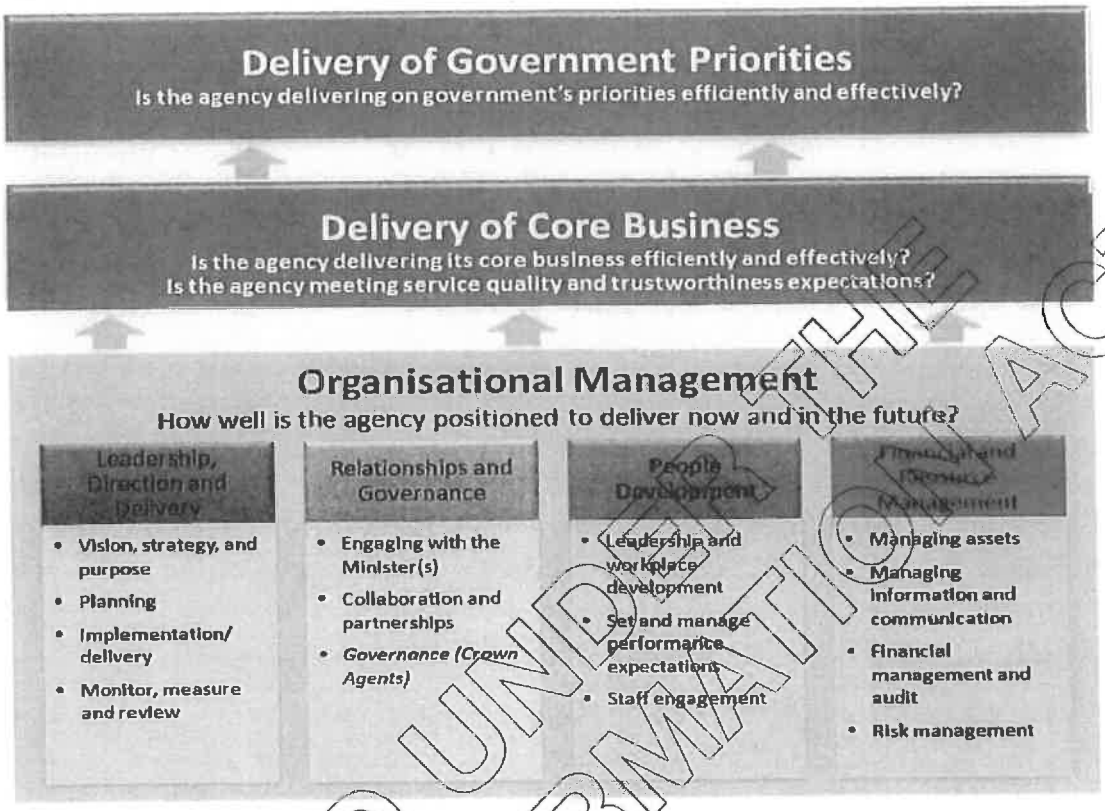
11 Executive leadership teams in the agencies recognise the need for performance improvement in the development areas.

12 The self assessment results also highlight opportunities for the agencies to draw on each other's differential strengths. Greater collaboration could mitigate individual and sector risks and improve sector performance. In particular:

- the three executive leadership teams could focus on sector-wide business improvements by sharing outcomes, aligning performance measures and enhancing performance reporting
- steps could be taken to embed a culture of efficiency and effectiveness in each organisation
- a consolidated work plan identifying priority areas for performance improvement could be developed and implemented.

13 The priority areas should be seen as a basis for shared work. The real benefits will be realised from taking a sector focus which recognises the inter-relationships between the drivers of performance improvement and the actions that are targeted.

Figure 1: Performance Improvement Framework (PIF) tool used to for self assessments



Each critical area has a number of elements which contain lead questions. The Framework enables each area to be assessed and scored.

Scoring System

Results: Direction of Travel

↔	Performance Maintained
↑	Performance Improving
↓	Performance Deteriorating
●	Performance Data Unavailable

Organisational Management: Traffic Lights

Blue	Strong – agency has a high level of capability now and is well positioned for the future.
	Well placed – agency has a good level of capability.
Amber	Development area – agency has some weaknesses in capability but robust strategies are in place to address areas of concern.
Red	Serious concern – significant weaknesses that require urgent action.

Scoring System Application

s.6(a)

[redacted]

Figure 2: Summary of delivery results

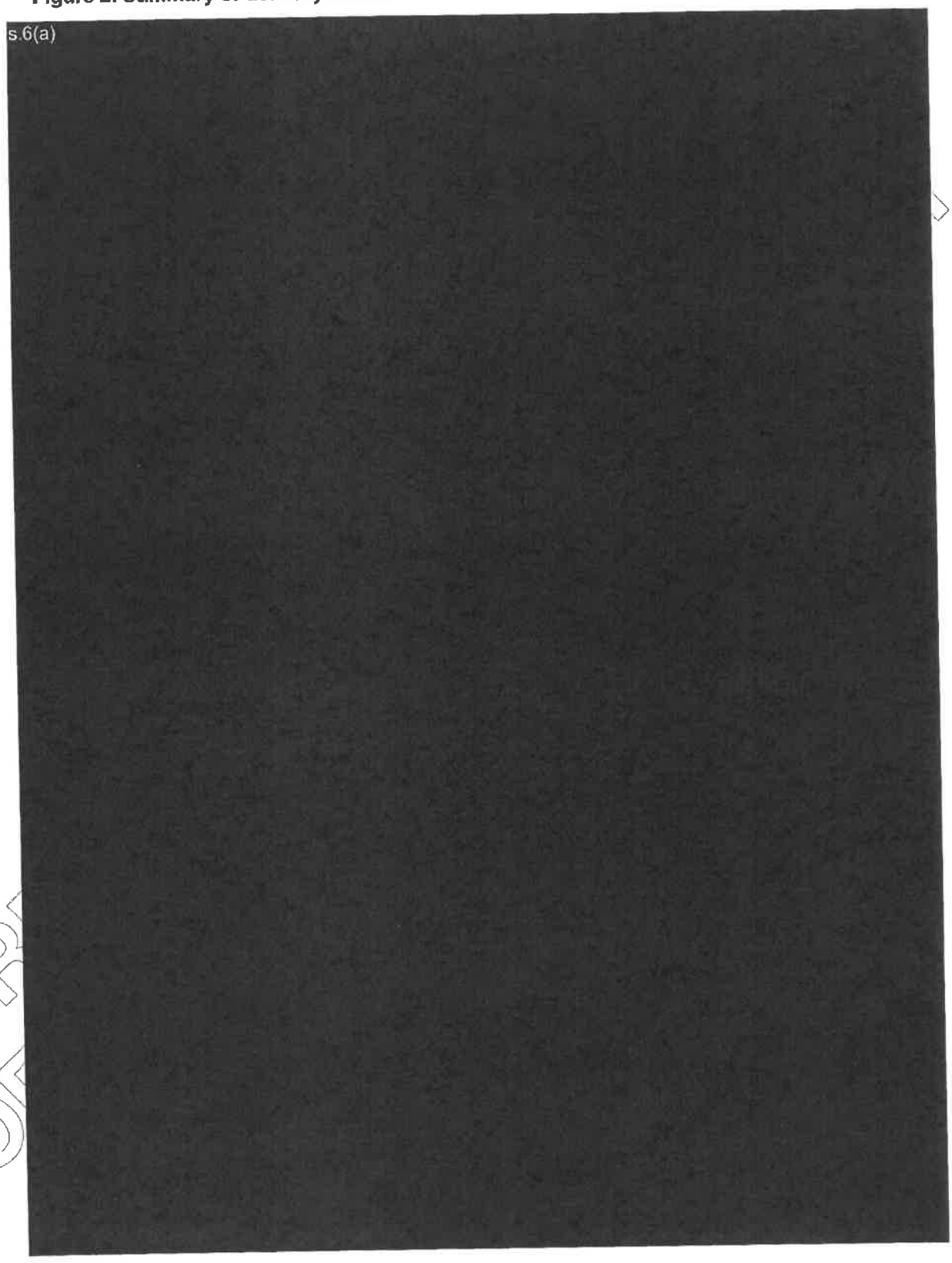
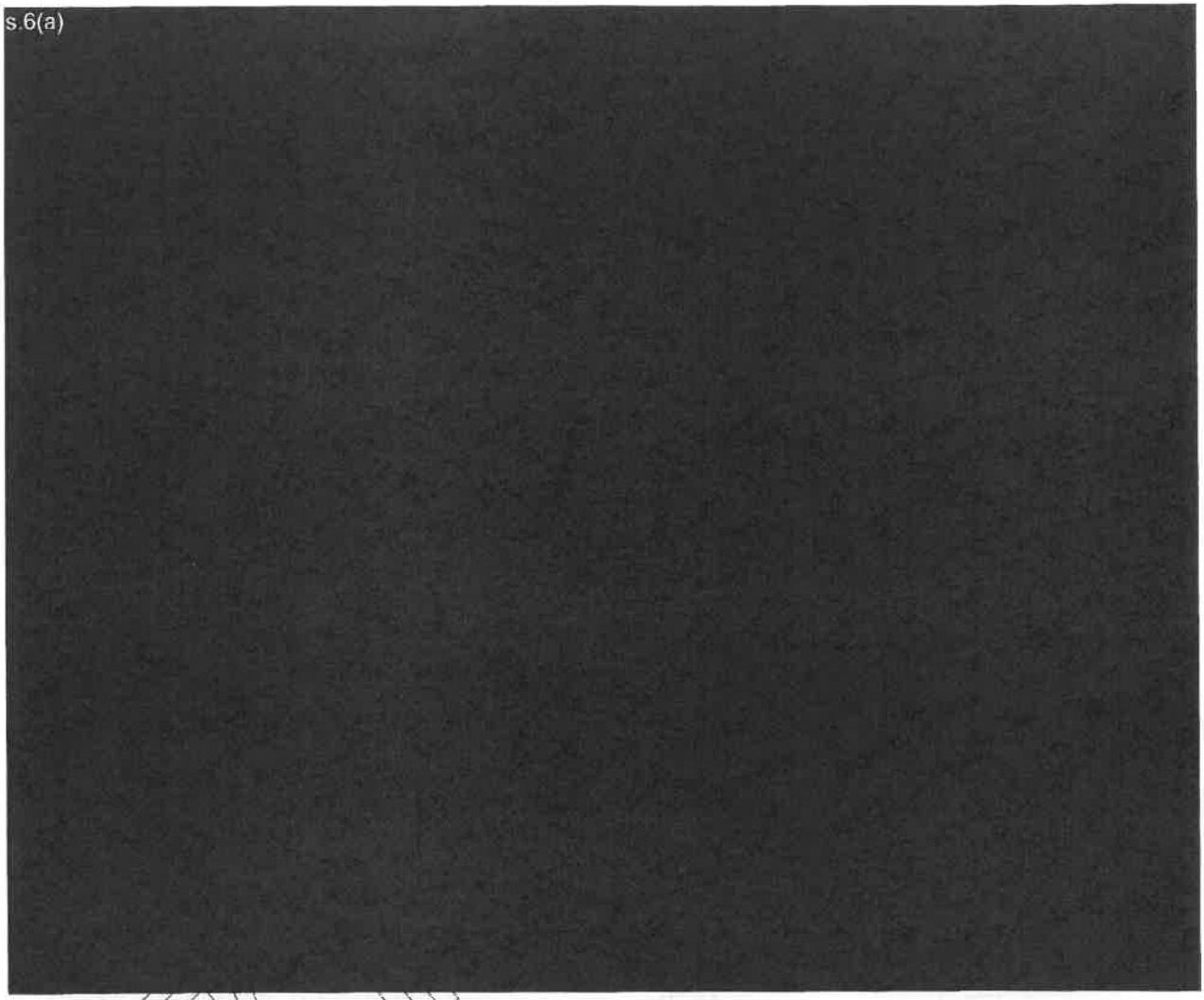


Figure 3: Summary of organisational management results

s.6(a)



Annex 9: People Interviewed or Consulted During the Review

Intelligence Agencies

s.9(2)(a) [redacted]

s.9(2)(a) [redacted]

Central Agency Chief Executives

- Iain Rennie (State Services Commissioner)
- Maarten Wevers (Chief Executive, DPMC)
- John Whitehead (Chief Executive, Treasury)

s.9(2)(a) [redacted]

Annex 10: Glossary

CCIP	Centre for Critical Infrastructure Protection
CTAG	Combined Threat Assessment Group
DDIS	Directorate of Defence Intelligence and Security
DES	Domestic and External Security
DESG	Domestic and External Security Group
DESS	Domestic and External Security Secretariat
DPMC	Department of Prime Minister and Cabinet
EAB	External Assessments Bureau
GCSB	Government Communications Security Bureau
GEOINT	GeoSpatial Intelligence
IA	Information Assurance
MFAT	Ministry of Foreign Affairs and Trade
NAC	National Assessments Committee
NMCC	National Marine Coordination Centre
NZDF	New Zealand Defence Force
NZIC	New Zealand Intelligence Community
s.6(a)	[redacted]
NZSIS	New Zealand Security Intelligence Service
NZSOC	New Zealand SIGINT Operations Centre
ODESC	Officials' Domestic and External Security Committee
ODESC(G)	Officials' Domestic and External Security Committee (Governance)
ODESC(I)	Officials' Domestic and External Security Committee (Intelligence)
ODESC(P)	Officials' Domestic and External Security Committee (Policy)
UN	United Nations